KASPERSKY LAB

Kaspersky® Internet Security 6.0

使用手册

目錄

一、 前言

Kaspersky® Internet Security 6.0 是完全的整合式解決方案，可使您的電腦防止來自網際網路的所有主要威脅，包括病毒、駭客攻擊、垃圾信件與間諜軟體。近來，個人電腦處在來自混合式威脅的最危險狀態，且人們所稱的'地下犯罪' 隨著網際網路普及而漸增。因此，防毒軟體已經不足以完全保護您的電腦。

Kaspersky Internet Security 6.0 結合來自卡巴斯基實驗室(Kaspersky Lab)的最新科技發展以防護惡意程式碼、阻擋網路攻擊及過濾垃圾信件。所有產品元件可緊密整合，避免系統衝突及確保您電腦高速操作。

主要優勢

防衛電腦的聯合陣線：Kaspersky Internet Security 6.0 可在您的電腦上處理所有進出的資料，包括電子郵件、網際網路流量與網路上的互動。不需要其他應用程式即可完全保護您的電腦。

相容性：此產品的主要優點是它與來自 Microsoft Windows 系列(包括 Microsoft Windows x64)的作業系統完全相容，並能與 Microsoft Windows XP 資訊安全中心整合。基於 Intel Centrino 行動運算技術提供筆記型電腦最佳化的效能，並支援 HT 技術的 Intel 處理器電腦最佳化運算 。

簡易和方便：初始設定精靈可幫助您選取程式的最佳操作模式，常態的防毒資料庫和程式自動更新，且相關輔助說明使您可迅速了解此產品最佳設定方式。

Kaspersky Internet Security 6.0 提供：

病毒防護

電子郵件保護：根據經由在任何郵件程式上傳送的協定(POP3、IMAP 和 NNTP 用於內收郵件，而 SMTP 用於外寄郵件)來進行電子郵件流量的防毒掃描。我們可為流行的郵件程式、Microsoft Outlook 和 Microsoft Outlook Express 在郵件資料庫中進行防毒和解毒處理。

網際網路流量掃描：可進行所有 HTTP 網際網路流量的即時防毒掃描，表示當物件儲存在電腦應碟時，受感染的物件會被排除。Microsoft Internet Explorer 有害 Scripts 的外掛程式將會被直接攔截。

檔案系統保護：可掃描所有個別檔案、目錄與磁碟的病毒。而且，只要啟動 Microsoft Windows，可在作業系統與下載的物件的重要區域上進行掃描，以確保注意力著重在最可能受感染的區域與物件。

免疫防護：可不斷地監看在電腦的記憶體裡開始的程式活動、和處理程序。它可警告使用者任何有關危險物件、可疑和隱藏的處理程序(Rootkits 病毒程式)、避免檔案系統的有害破壞、及在惡意活動後暫存及復原系統至正常狀態。

防護間諜軟體

保護機密資訊：此產品可避免使您的機密資訊(例如密碼、銀行帳號與信用卡片詳細資料)外洩。它可攔截網路釣魚詐欺信件，並警告您連結到使用社交工程方法來欺騙使用者提供例如登入、密碼或者存取網路銀行資訊的機密資訊的網路釣魚詐欺網站。

安全無虞的網路瀏覽：此產品可避免在網站上啟動危險的處理程序，並可阻斷妨礙系統正常運作的物件，而且使惡意程式碼進入您電腦的彈跳式視窗與網頁廣告。

攔截自動撥接程式：此產品可識別及攔截嘗試使用您的數據機來撥接付費電話服務的程式。

防護電腦駭客

攔截網路攻擊：此產品可在網路攻擊前來偵測掃描對您電腦連接埠刺探行為，並透過阻斷嘗試攻擊的連線來阻絕一般類型的駭客攻擊。網路活動將被即時監看以提供所有網路連接上相關的統計性資訊。

網路活動的完全控制：此產品根據設定的程式規則來控制從應用程式連接到各種不同網路的來源請求、以及追蹤所有內送和外傳的資料封包。

進行所有網路的安全運作：當電腦連接到網路時，程式允許使用者指定網路的類型(信任網路、企業網路或網際網路)，所以防火牆可選擇規則的嚴格性。

提供線上隱藏模式：此模式可避免您的電腦被在網際網路上的其他電腦看見。只要您已轉變成此模式，除了在例外規則裡的指定之外，所有的外部向本機的連線都會被停止。

垃圾郵件過濾

整合式的垃圾郵件過濾方法：多種方法組合以確保垃圾信件最高的偵測能力包含：電子郵件地址的黑名單和白名單(包括網路釣魚網站的 URLs)與在訊息文字中的片語清單、以及使用自學演算法的訊息文字分析。此產品也可以偵測圖像方式的垃圾信。

共同郵件程式的支援：特別設計用於 Microsoft Outlook、Microsoft Outlook Express 和 The Bat！的擴充模組允許您根據分析狀態來設定訊息的處理規則。

訊息的初步分析：為了要避免浪費時間與網路流量，使用者可在從郵件伺服器下載前，進行所有內送電子郵件的訊息標題初步分析。此方式可減少下載到您電腦的垃圾信與病毒的風險。

二、 安裝環境需求

一般需求：

§ 50 MB 可用硬碟空間
§ CD-ROM (供使用 CD 來安裝 Kaspersky Internet Security 6.0)
§ 網際網路連接 (用以將產品啟動)
§ Microsoft Internet Explorer 5.5 或更高版本 (經由網際網路更新防病毒資料庫與程式模組)

系統需求：

Microsoft Windows 98 (SE)
§ Intel Pentium 133 MHz 或同等 CPU
§ 64 MB RAM

Microsoft Windows ME:
§ Intel Pentium 150 MHz 或同等 CPU
§ 64 MB RAM

Microsoft Windows NT Workstation 4.0 (具 Service Pack 6a)：
§ Intel Pentium 133 MHz 或同等 CPU
§ 64 MB RAM

Microsoft Windows 2000 Professional (with Service Pack 2 或更高版本)
§ Intel Pentium 133 MHz 或同等 CPU
§ 64 MB RAM

Microsoft Windows XP Home Edition
§ Intel Pentium 300 MHz 或同等 CPU
§ 128 MB RAM

Microsoft Windows XP Professional x64 Edition
§ Intel Pentium 300 MHz 或同等 CPU
§ 128 MB RAM

三、 安裝說明

步驟 1：

在 kis6en.msi 上按右鍵，選取“安裝”。

（PS：建議將授權金鑰和安裝程式置於 C 碟機下同一資料夾內）

步驟２：

接下來為歡迎畫面，請選擇 next。

步驟３：

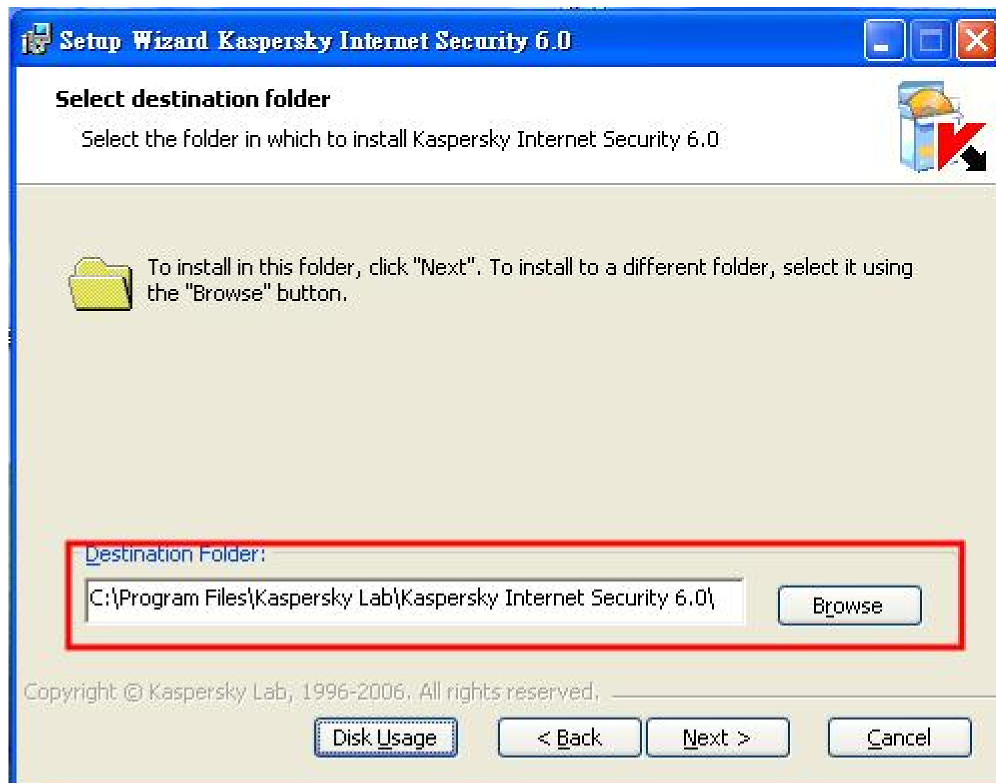
選取【I accept the terms of the License Agreement】，請選擇 next。



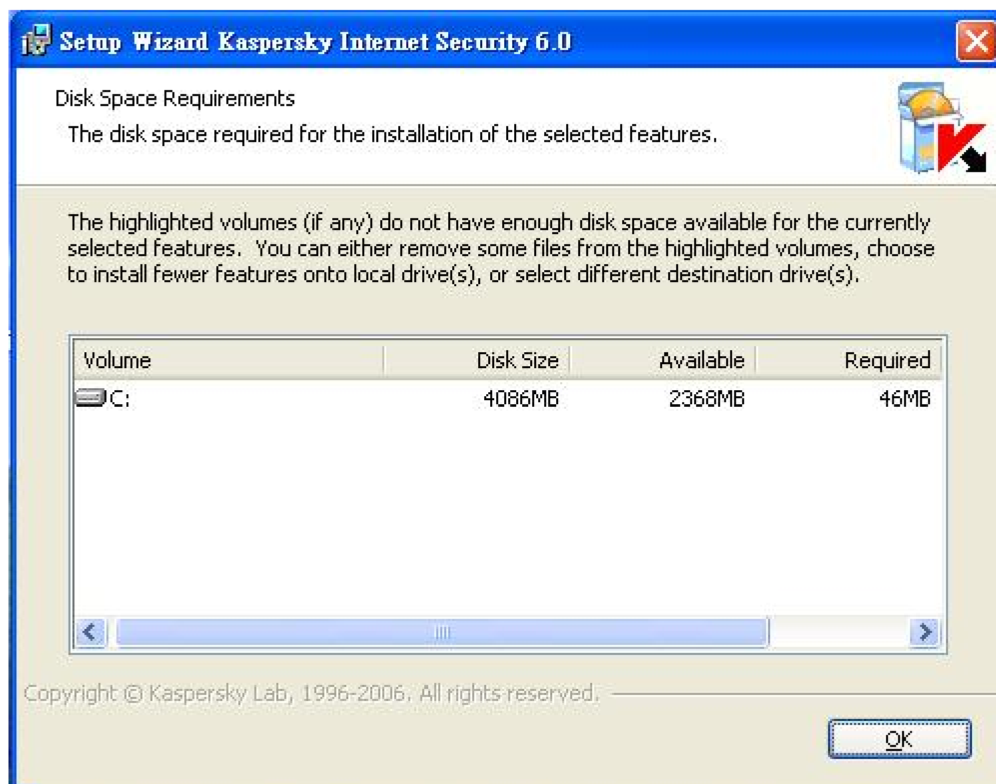
步驟４：

建議安裝卡巴斯基防毒軟體 6.0 於預設路徑（若要安裝於不同路徑，請按【瀏覽】）請選擇 next。

（Disk Usage：查看磁碟空間，見**步驟４－１**）

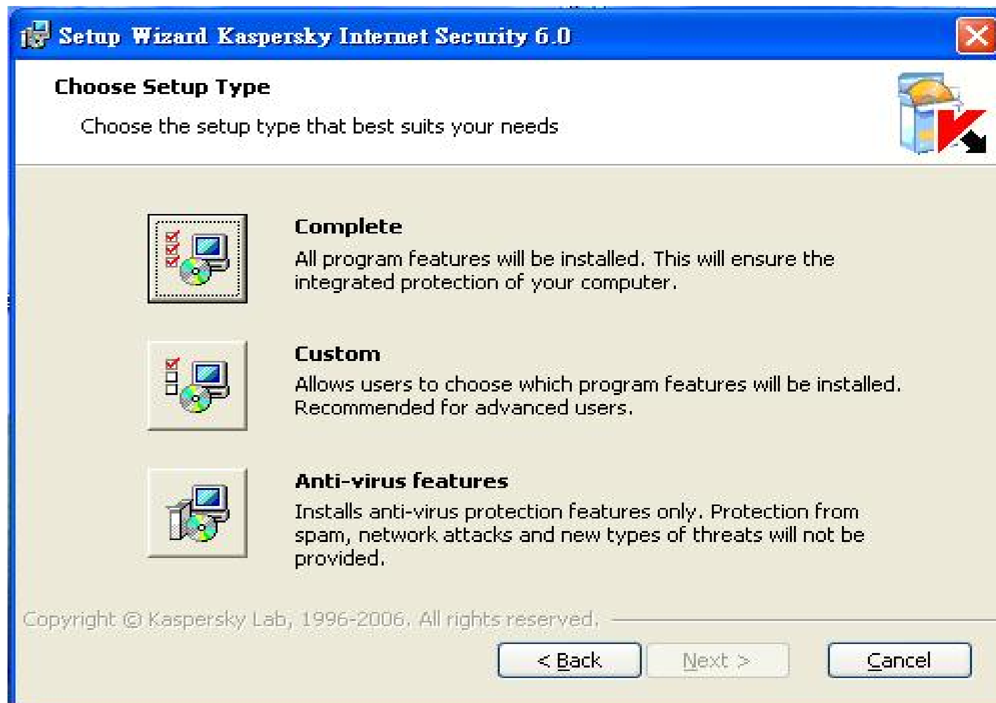


步驟４－１：



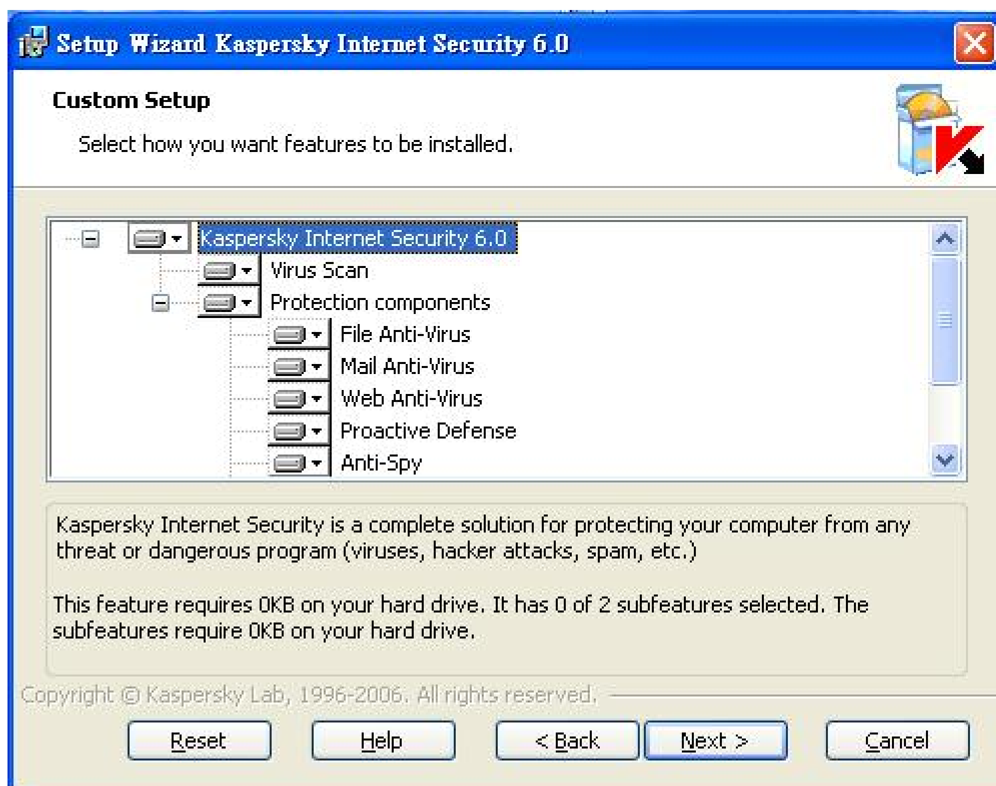
步驟５：

選擇安裝類型【完整安裝】或【自訂安裝】 （見**步驟**５－１）或【僅安裝防毒功能】。(不安裝垃圾郵件，網路攻擊保護及新型態威脅保護)(跳至**步驟**７)



步驟５－１：

自訂所要安裝的元件，請選擇 next



步驟6：

預設為 Disable Windows Firewall：不啟用 windows 內建防火牆避免與 Kaspersky Anti Hacker Firewall 相衝突，請選擇 next



防毒軟體將進行開始安裝程序請隨著安裝精靈指示進行安裝

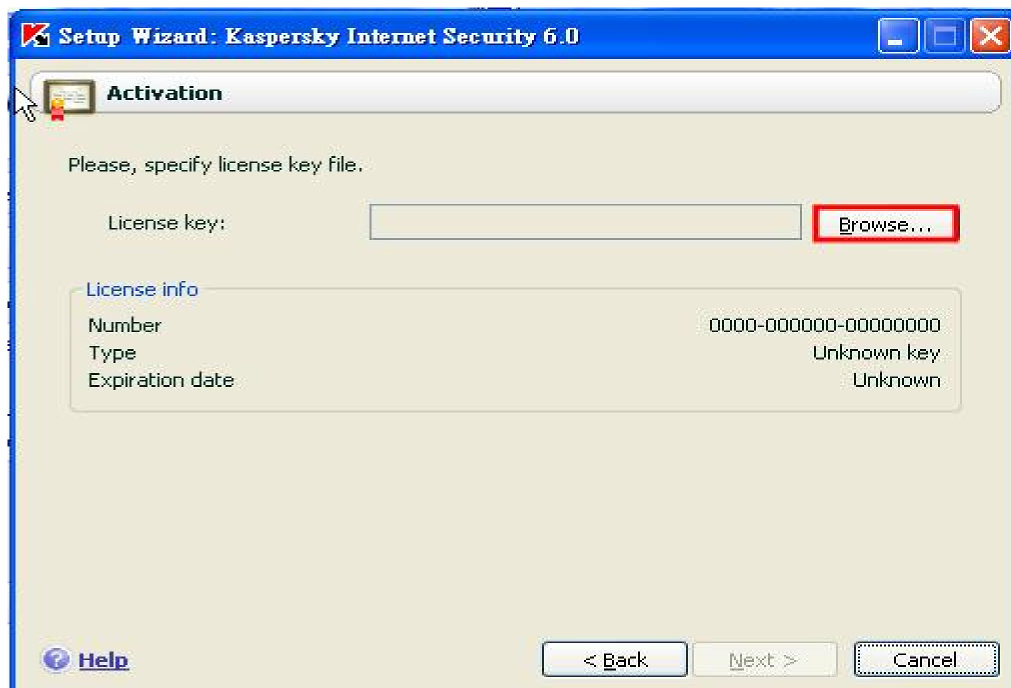
步驟 7：

選擇啟動卡巴斯基防毒軟體的方式，預設為使用【Activate using the activation code】:使用啟動碼，目前建議使用者改為【Apply existing license key】:使用授鑰金鑰



步驟 8

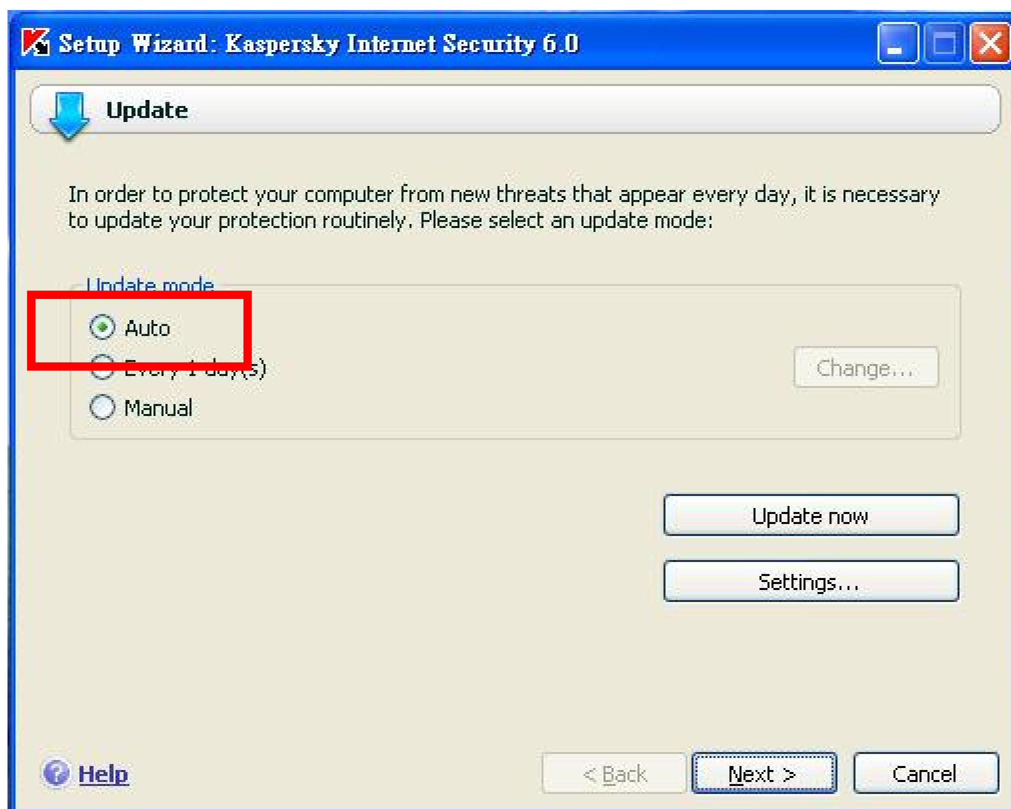
按【瀏覽】選取授權金鑰所在的位置，點選授金鑰，再按開啟，即可看見授鑰資訊，然後請選擇 next



授權金鑰驗証成功後，即可看見授權資訊，然後請選擇 next

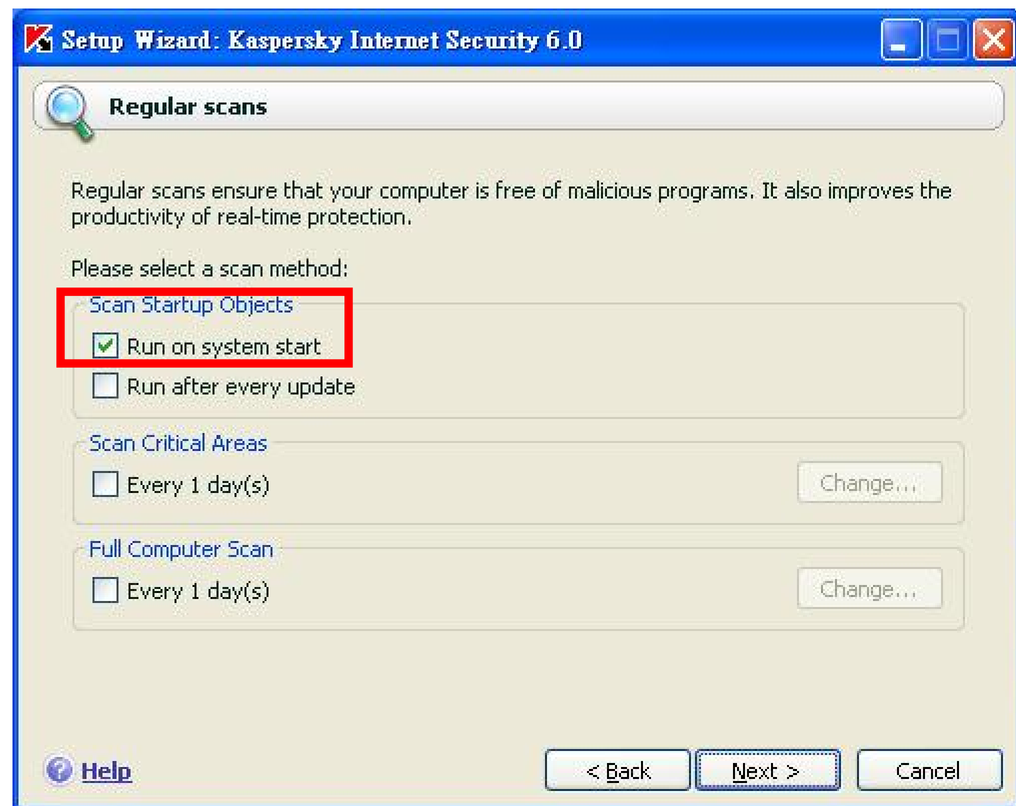
步驟 9：

設定更新方式，預設為【Auto】：自動更新(建議使用)然後請選擇 next



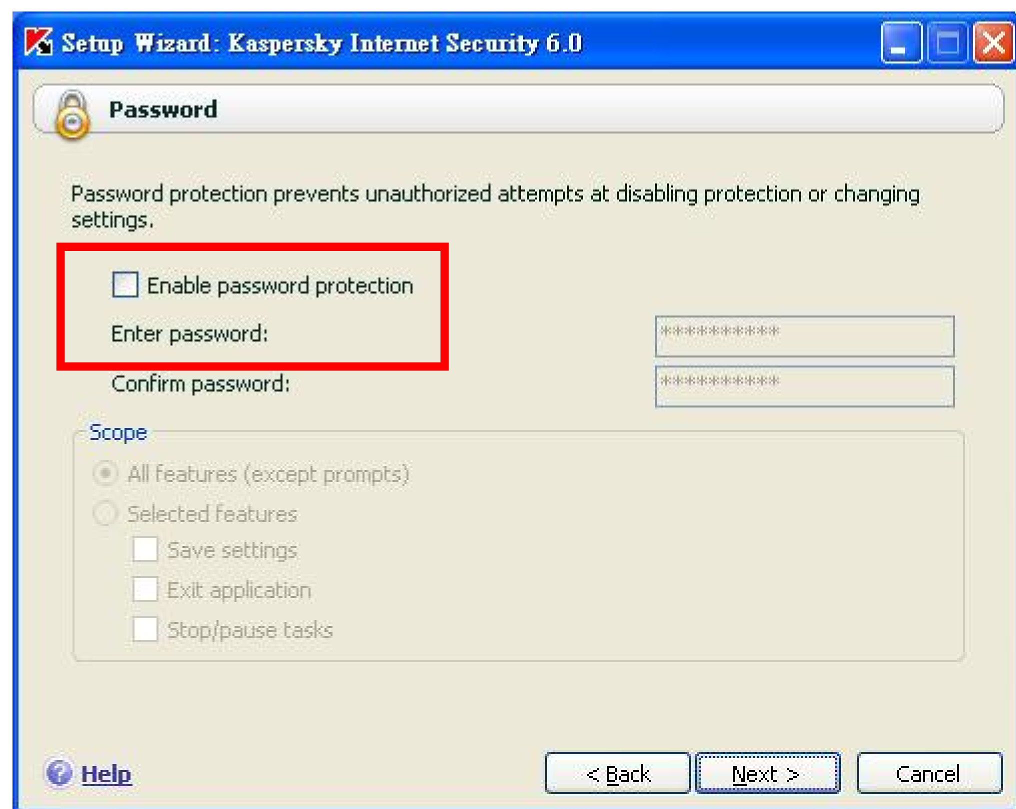
步驟 10：

掃描設定，預設為【Run on system start】：當系統啟動時執行，然後請選擇 next



步驟 11：

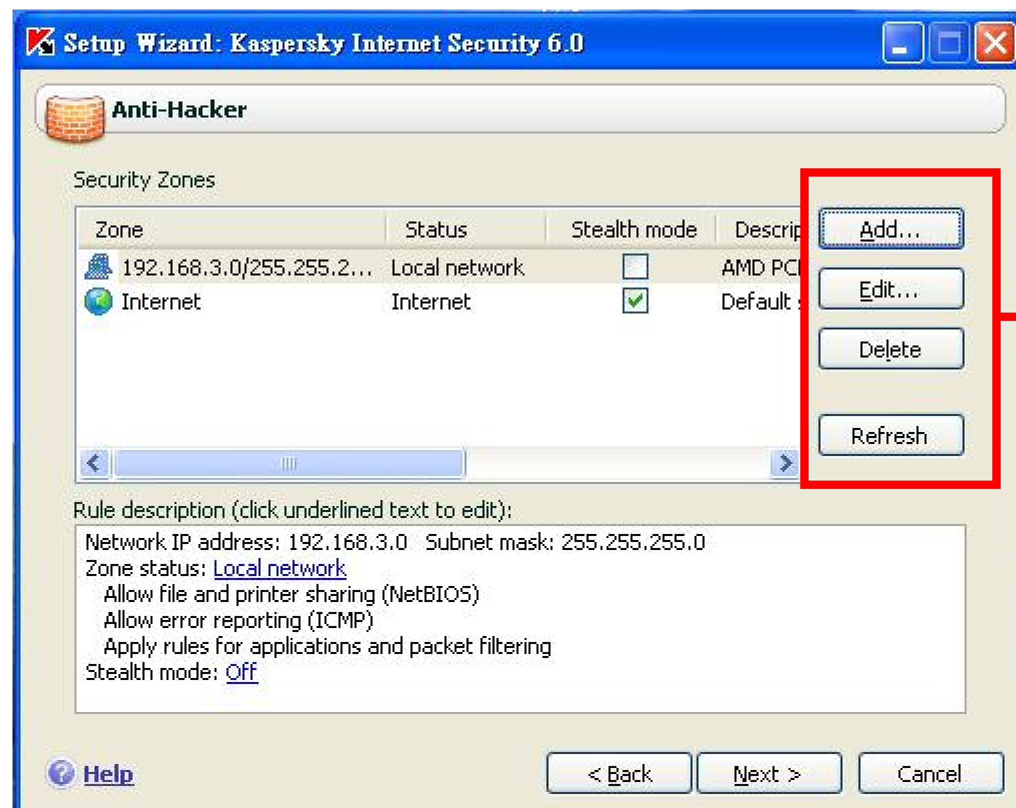
設定密碼保護，預設為【Enable password protection 不啟用】然後請選擇 next



步驟 12：

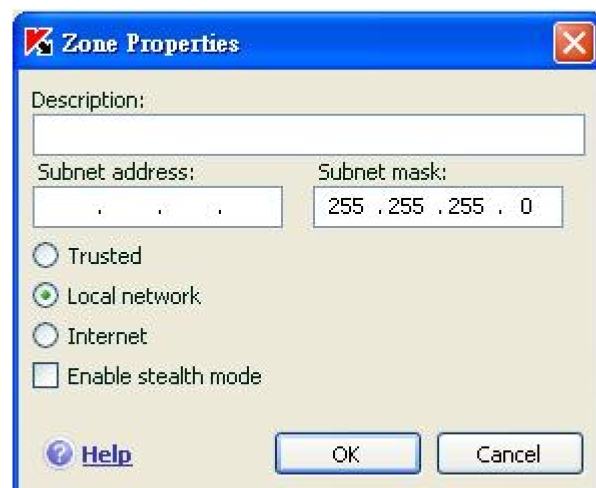
設定 Kaspersky Anti-Hacker Firewall，然後請選擇 next

（設定網段是否啟用隱形模式）



可在此做新增，編輯，刪除，更新的動作

Add：新增（使用者可新增自訂的網段，如圖）



Description：描述

Subnet address：網段 Subnet mask：子網路遮罩

Trusted：信任

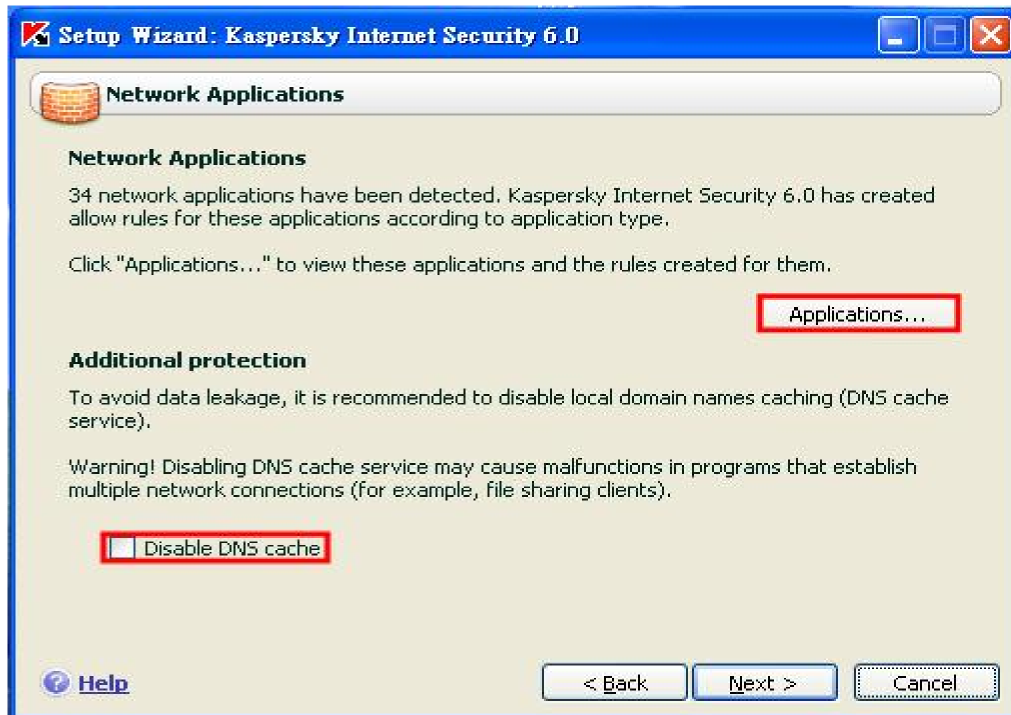
Local network：內部網路

Internet：網際網路

Enable stealth mode：啟用隱形模式

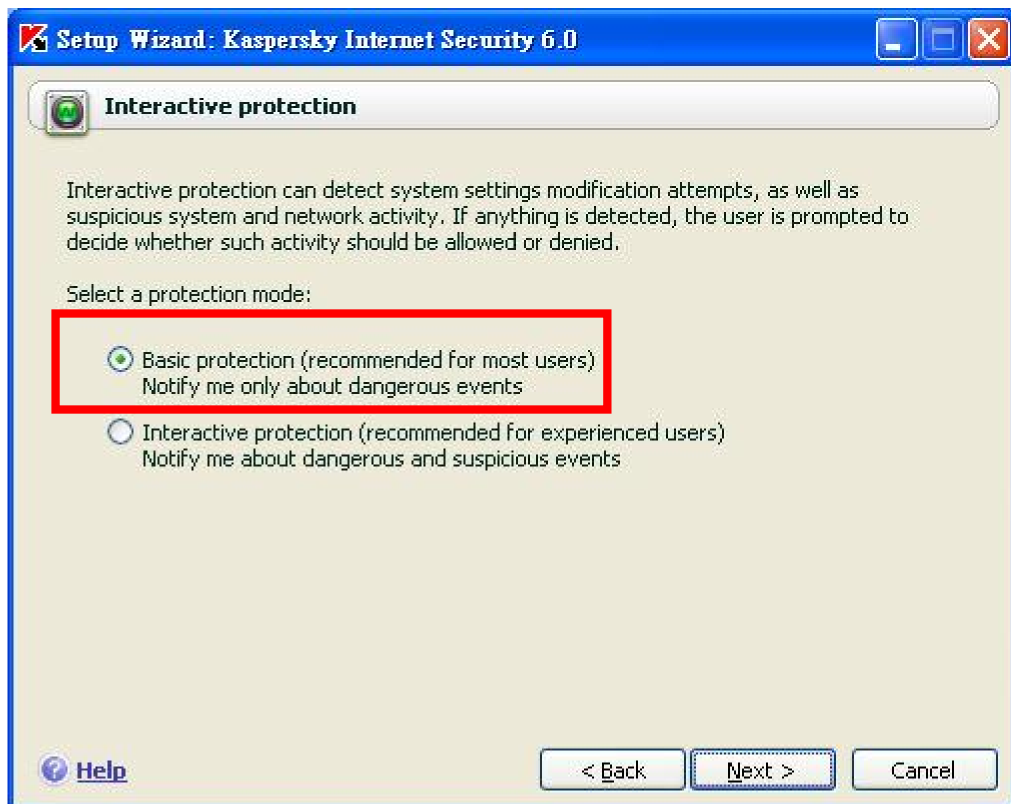
步驟 13：

設 Firewall 應用程式規則，可再此選項設定應用程式，也可稍後在設定，以及預設為【Disable DNS cache】:不啟用 DNS 快取，然後請選擇 next



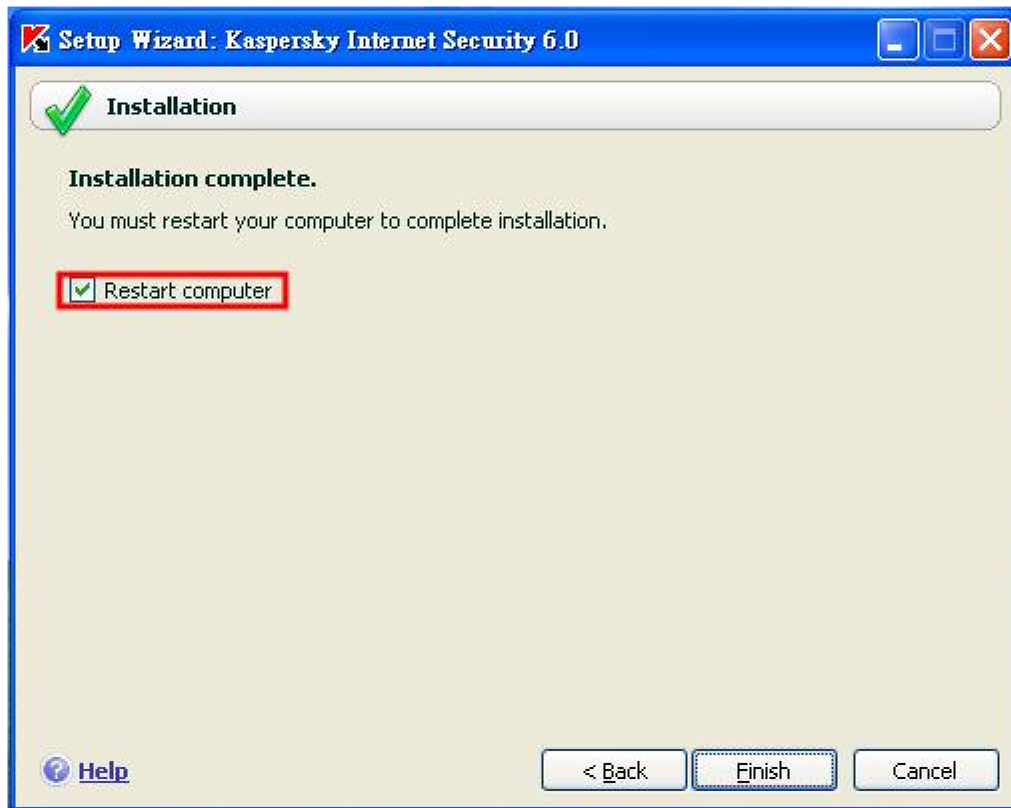
步驟１４：

設定免疫防護，預設為【Basic protection(recommended for most users)】：基本免疫防護，然後請選擇 next



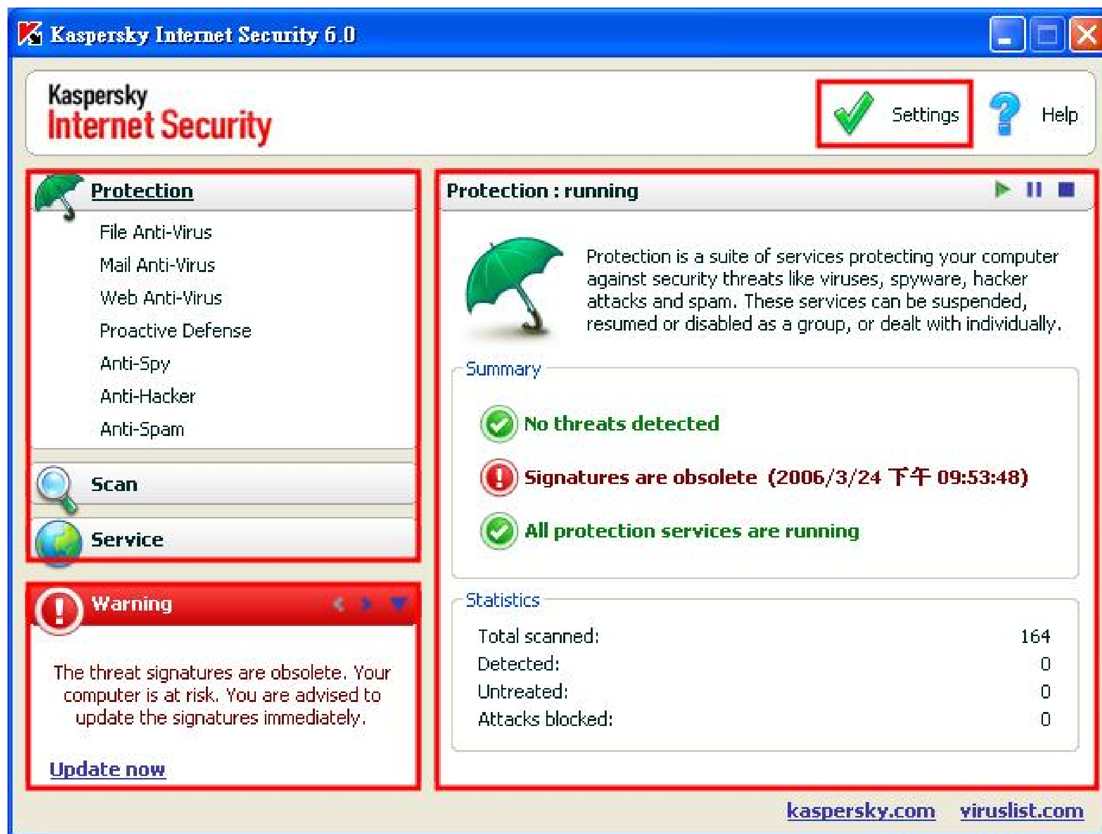
步驟１５：

安裝完成，預設為【Restart computer】：重新開機，然後請選擇 Finish



四、 一般操作

Protection



左邊為功能區：

分為 Protection、Scan、Service。顯示卡巴斯基主要防護功能

左下方訊息區：

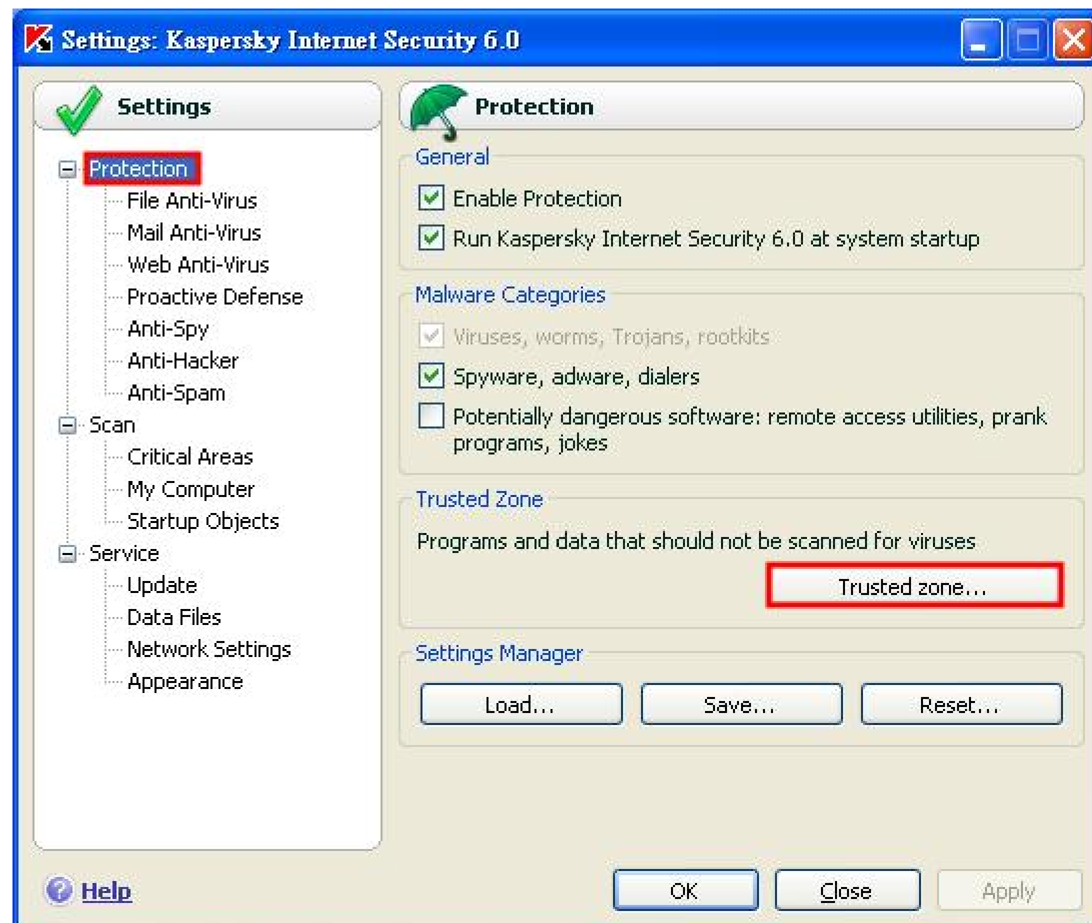
提醒使用者正在執行的工作

右邊為功能操作區：

包含執行狀態及統計資訊

如果要使用修改設定時，可利用畫面上方【設定 Setting】進入進階設定畫面

Settings- Protection



General

Enable Protection：啟用防護功能

Run Kaspersky Internet Security 6.0 at system startu：開機後自動執行 KIS6.0

Malware Gategories

Viruses.worms.Trojans.rootkits：開啟對病毒、蠕蟲、木馬、rootkits 的防護

Spyware.adware.dialers：開啟對間諜程式、廣告程式、撥接程式的防護

Potentially dangerous software:remote access utilities.prank program.jokes：潛在的危險軟體

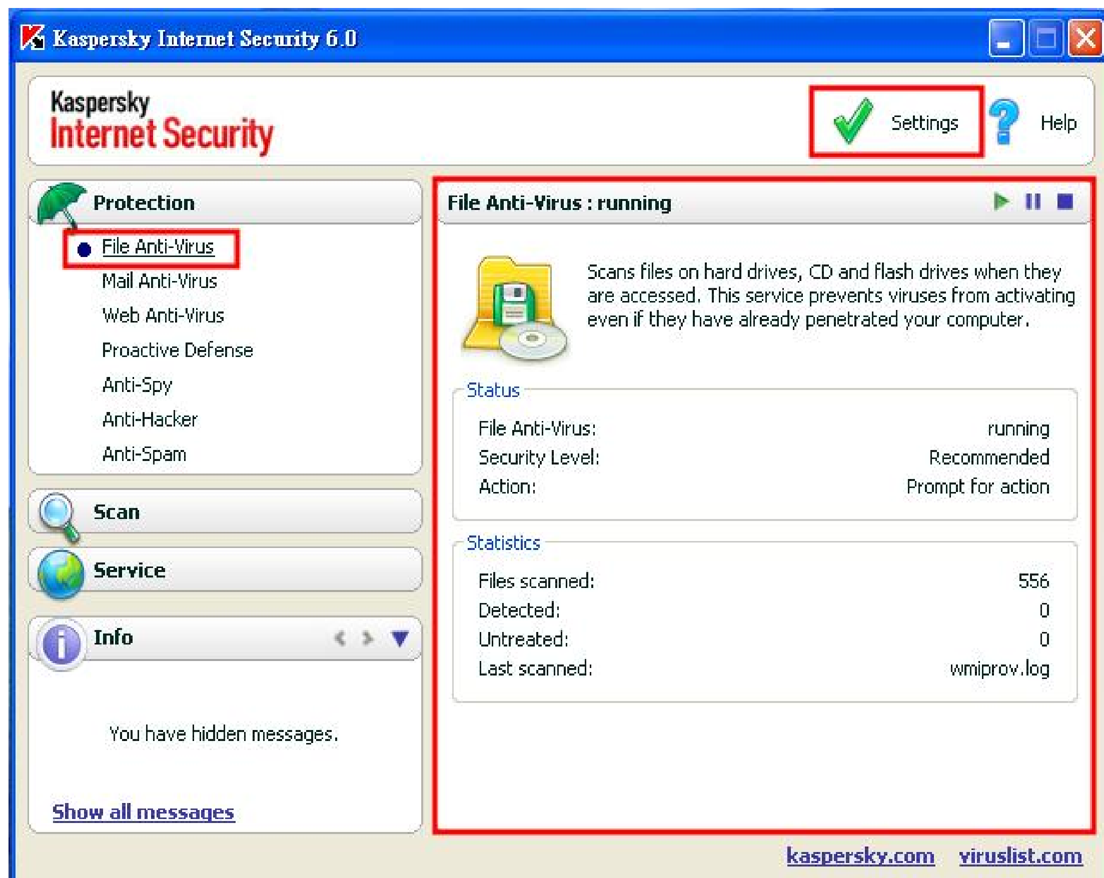
Trusted Zone

可以將特定的程式或是資料排入信任的清單中，如此在掃描病毒的時候可以跳過這些項目。

Settings Manager

卡巴斯基設定檔及規則的管理。

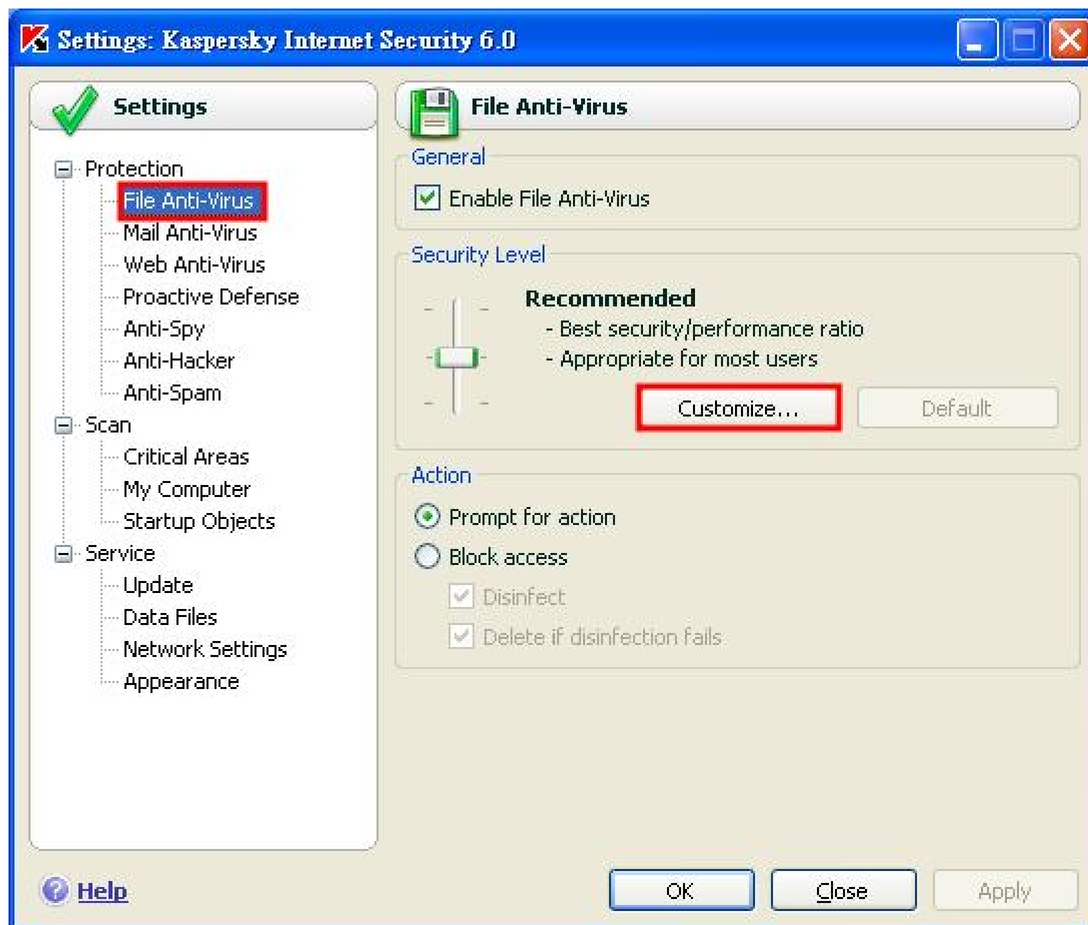
File Anti-Virus (檔案防護)



畫面右邊會顯示執行狀態、保護等級及偵測到病毒時的處理動作。

Statistics：顯示保護檔案數、病毒偵測數及最後掃描的檔案等相關統計資訊

Settings- File Anti-Virus (檔案防護)



General

Enable File Anti-Virus：預設是啟動的狀態，來監控文件(檔案)的部份

Security Level

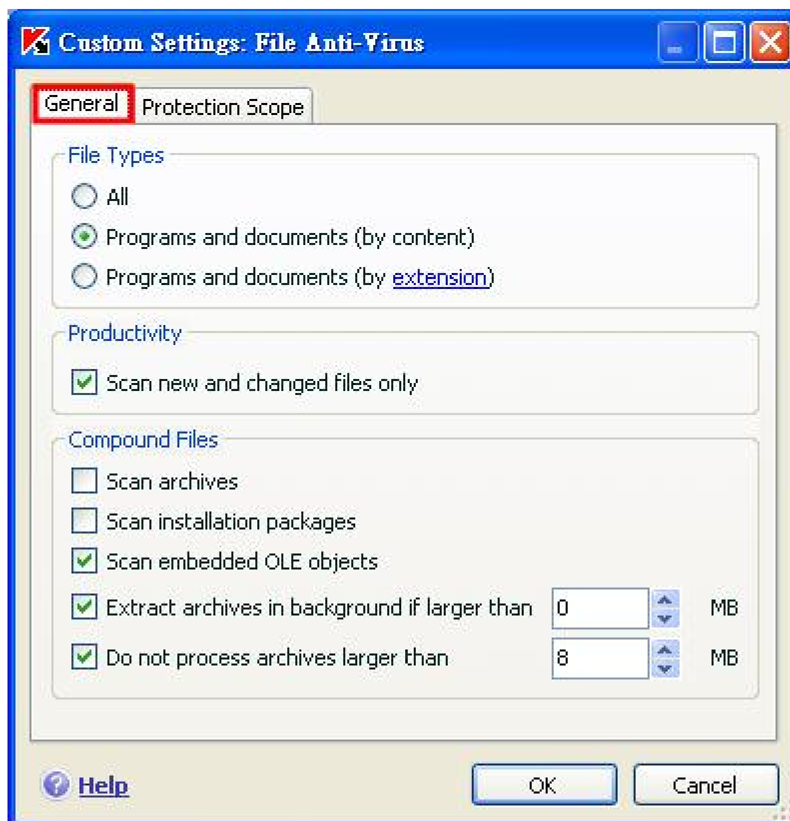
預設是中等的狀態即可，且對於檔案監控較詳細的設定，可以點選此處的customize

Action

Prompt for action：如果檔案有問題，會出現訊息視窗詢問使用者

Block access：預設執行動作如果掃描到病毒則清除病毒，如果無法清除病毒則刪除檔案

File Anti-Virus-Customize[Genernal]



FileType

All：掃描全部檔案

Programs and documents(by content)

Programs and documents(by extension)

Productivity

只掃描新的並且改變的檔案（此預設選項卡巴斯基在下次的即時檔案防護會對於新增或是有修改過的檔案做掃描的動作）。

Compound Files

Scan archives：掃描檔案

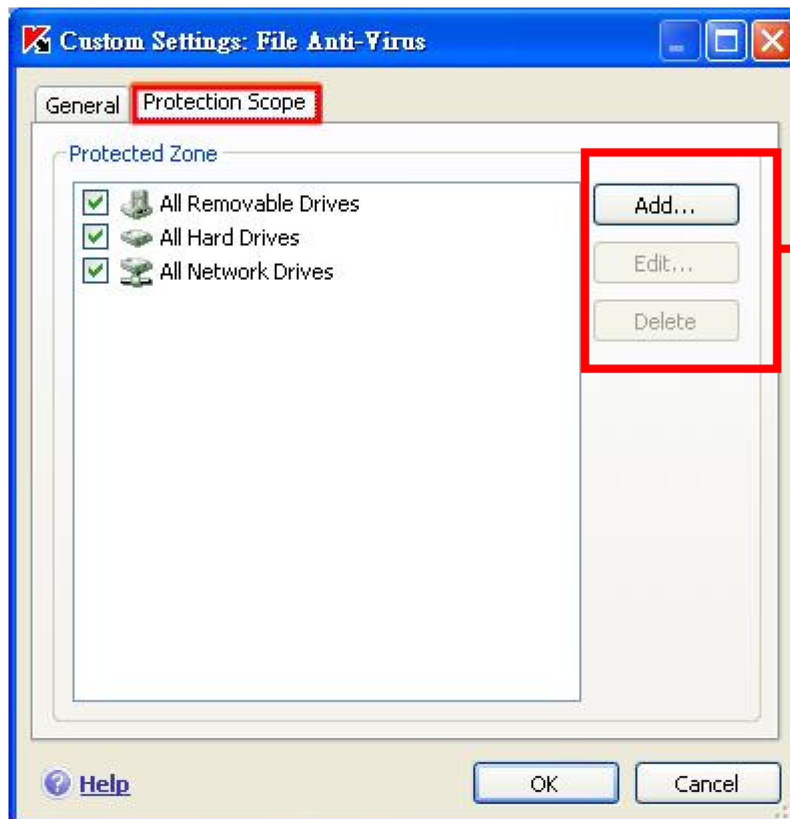
Scan installation packages：掃描安裝檔案

Scan embedded OLE objects：掃描嵌入 OLE 物件

Extract archives in background if larger then：擷取檔案於資料庫

Do not process archives larger then：不要處理大型檔案

File Anti-Virus-Customize[Protection Scope]



使用者可自行**增加**所要防護的區域，以及對於所選取的防護區域做**編輯**和**刪除**的動作

防護區域

All Removable Drives：隨身碟的週邊設備

All Hard Drives：電腦本身的磁碟機

All Network Drives：網路磁碟機

附註:使用者如果有做過內部的設定發生錯誤時，可以啟動預設的選項恢復原先安裝的文件監控狀態。

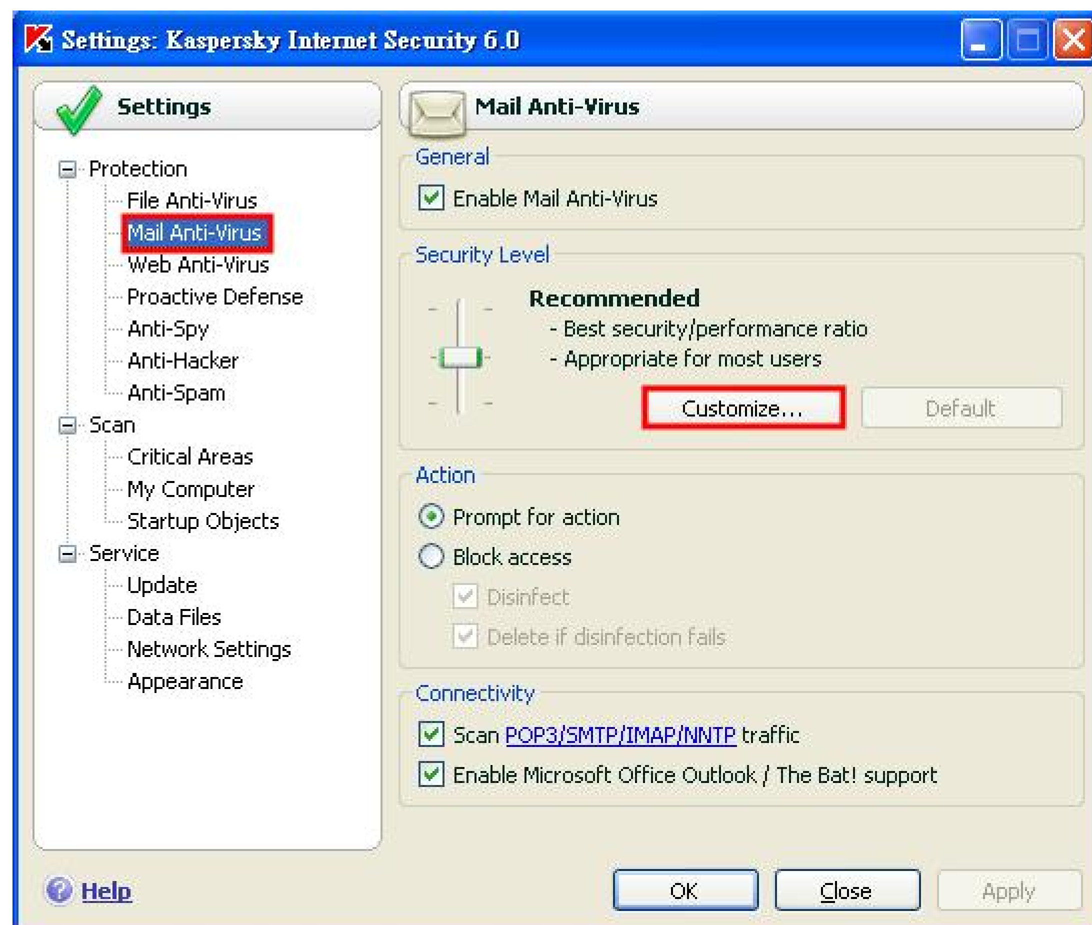
Mail Anti-Virus（郵件保護）



畫面右邊會顯示執行狀態、保護等級及偵測到病毒時的處理動作。

Statistics：顯示掃描物件數及病毒偵測數等相關統計資訊

Settings-Mail Auti-Virus



General

Enable Mail Anti-Virus：預設是啟動的狀態，來監控 Mail 的部份

Security Level

預設是中等的狀態即可，且對於 Mail 監控較詳細的設定，可以點選此處的 customize。

Action

Prompt for action：如果郵件有問題，會出現訊息視窗詢問使用者

Block access：預設執型動作如果掃描到病毒則清除病毒，如果無法清除病毒則刪除檔案

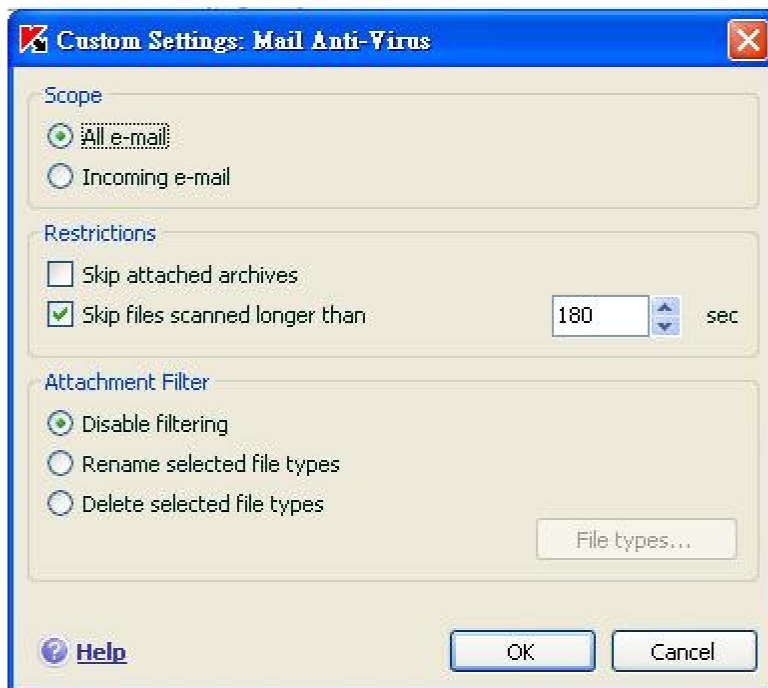
Connectivity

ScanPOP3/SMTP/IMAP/NNTP traffic：支援這些通信協定的掃描

Enable Microsoft Office Outlook/The Bat! Support：啟動 Microsoft Office Outlook 的郵件即時監控以及支援 The Bat 的郵件工具

附註:使用者如果有做過內部的設定發生錯誤時，可以啟動預設的選項恢復原先安裝的郵件監控狀態。

Mail Anti-Virus-Customize



Scope

All e-mail：預設對所有進入和進出的郵件做掃描

Incoming e-mai：指掃描進來的電子郵件

Restrictions

Skip attached archives：不掃描附件的檔案

Skip files scanned longer then…. 180sec：預設如果掃描檔案超過 180 秒則忽略

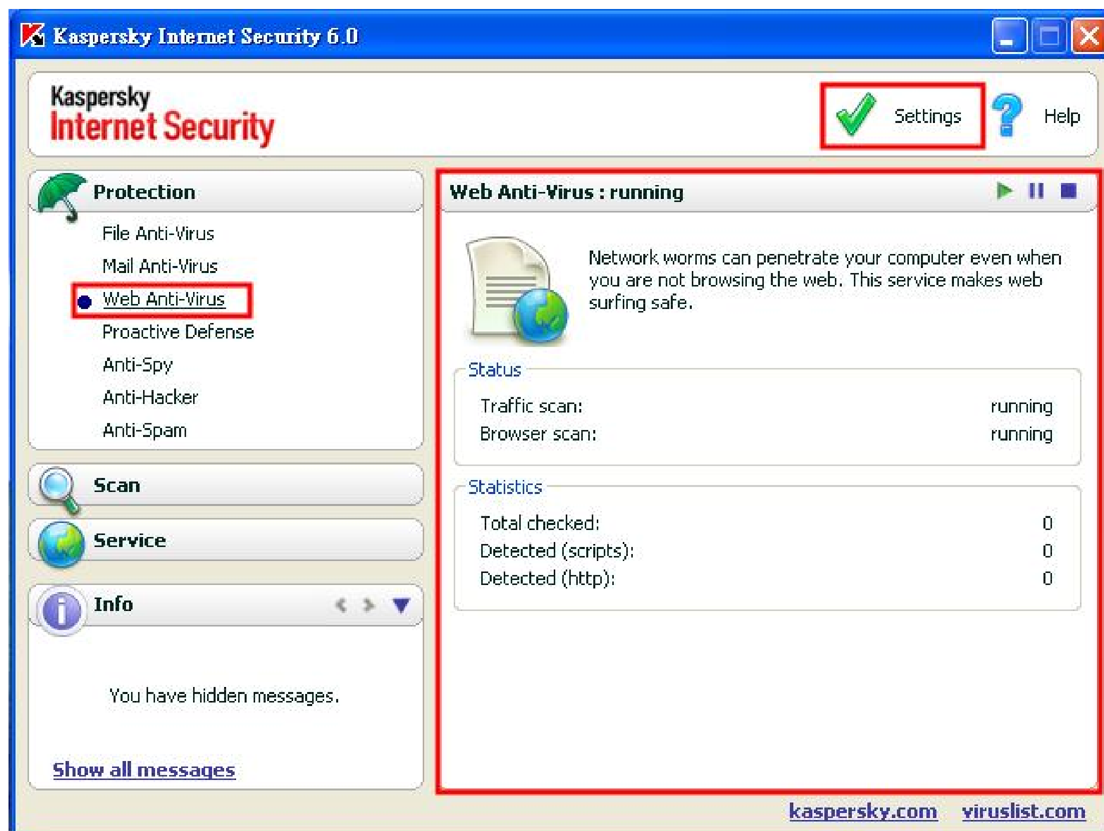
Attachment Filter

Disable filtering：預設停止電子郵件過濾

Rename selected file types：使用反斜線替原先的副檔名做更換副檔名的動作，可以使用文件類型中的檔案類型

Delete selected file types：可選擇直接刪除附加檔案的副檔名類型，可以使用文件類型中的檔案類型

Web Anti-Virus（網頁保護）



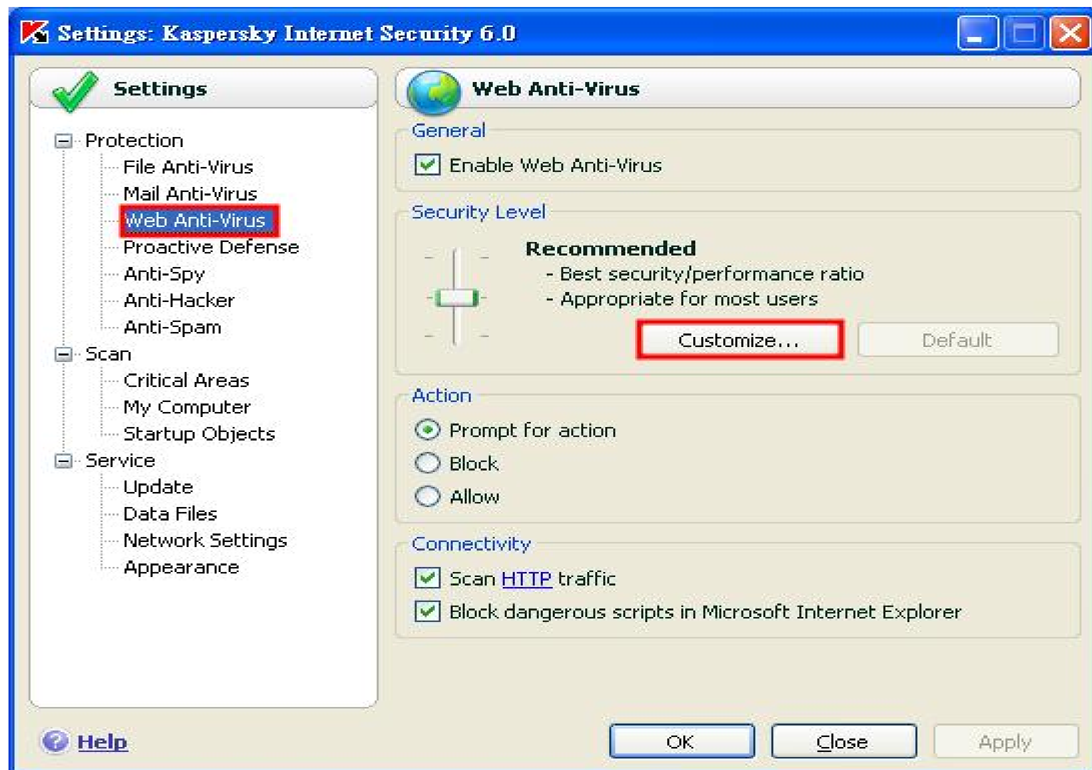
kaspersky Web Anti-Virus 提供使用者在網際網路上瀏覽網頁時，避免下載危險物件及透過網頁執行危險的 Script，提高使用者在瀏覽網頁時的安全。

右方狀態區：

Status：流量掃描及瀏覽掃描

Statistics：顯示目前所有掃描數量，包括 Script 及 Http

Settings- Web Anti-Virus（網頁保護）



Genernal

勾選為啟用 Web Anti-Virus，反之為不啟用。

Security Level

高：監控網頁上大部份的 Script 和 Object，以病毒資料庫的危險特徵進行完整掃描，建議使用在沒有使用其他 Http 安全工具的環境下

中（建議層級）：監控網頁上大部份的 Script 和 Object，利用掃描時間超過預設時間則停止掃描，以加速使用者瀏覽網頁的速度

低：建議使用在有安裝網頁保護軟體的電腦上，只掃描特定的 Script 及 Object

自訂層級：（見自訂層級操作）

Action

Prompt for action：提示使用者動作

Block：阻擋

Allow：允許

Connetivity

Scan HTTP traffic：勾選為啟用，反之為不啟用；點擊“HTTP”則請參考服務的網路設定

Block dangerous script in Micorosoft Internet Explorer：勾選為啟用，反之為不啟用，此項功能為阻擋 IE 的危險 script

Web Anti-Virus（網頁保護）-Customize

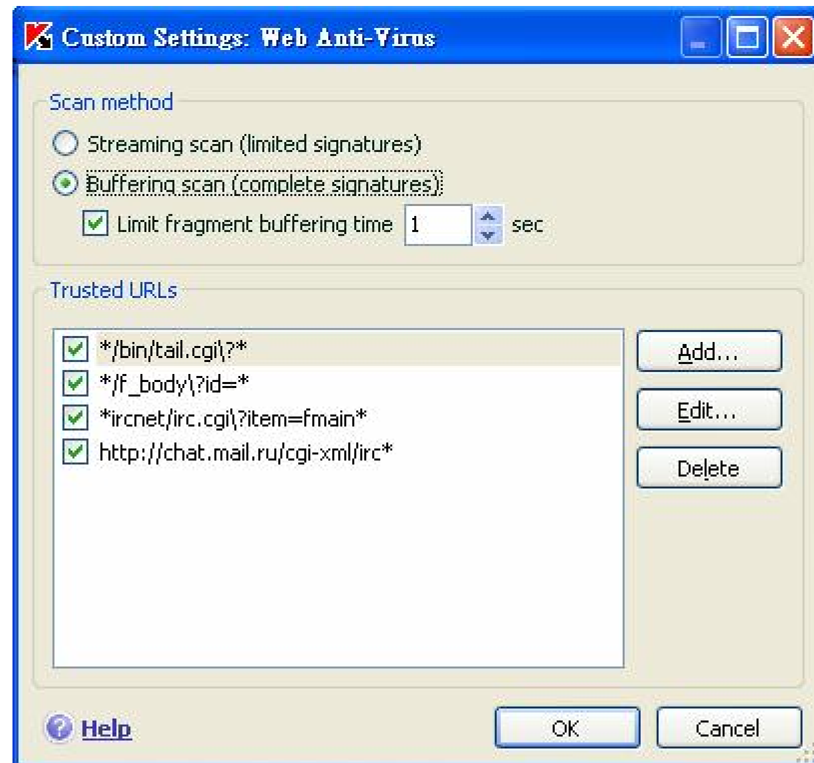
Scan method（設定掃描方式）

Streaming scan（limited signatures）：流量掃描，只掃描特定病毒特徵

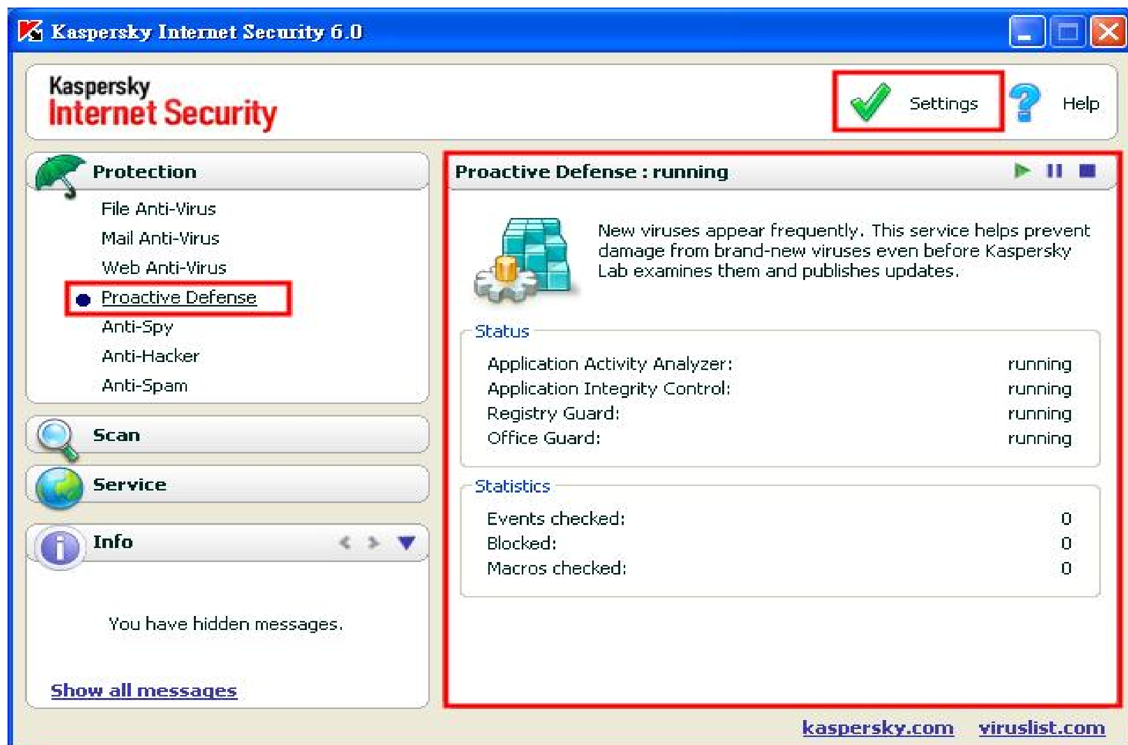
Buffering scan（complete signatures）：緩衝掃描，掃描全部病毒特徵

Limit fragment buffering time（sec）：超過指定緩衝掃描時間，則停止掃描

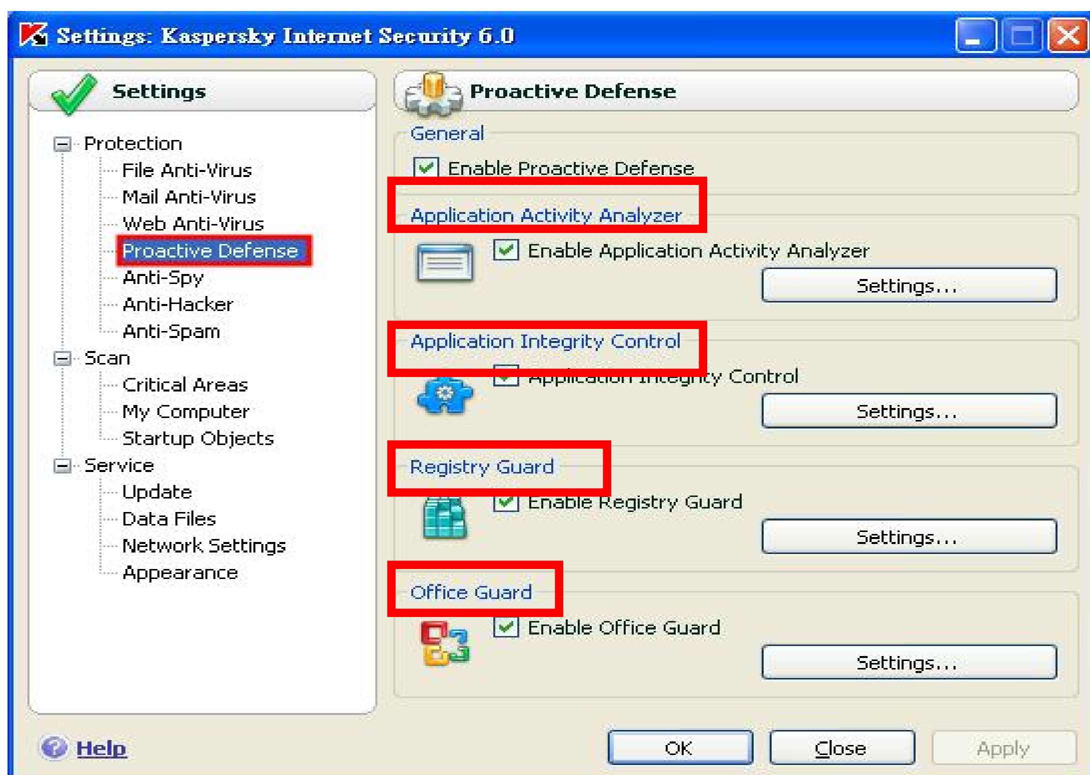
Trusted URLs：信任的 URL，此項僅建議進階使用者使用，提供使用者啟用、停用及新增、編輯、刪除 URL 規則



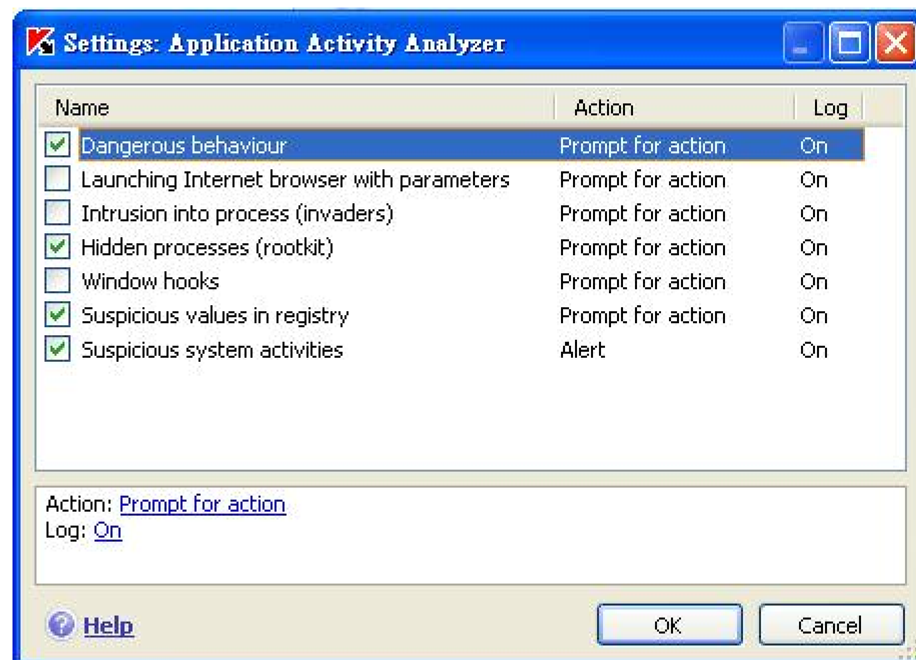
Proactive Defense(免疫防護)



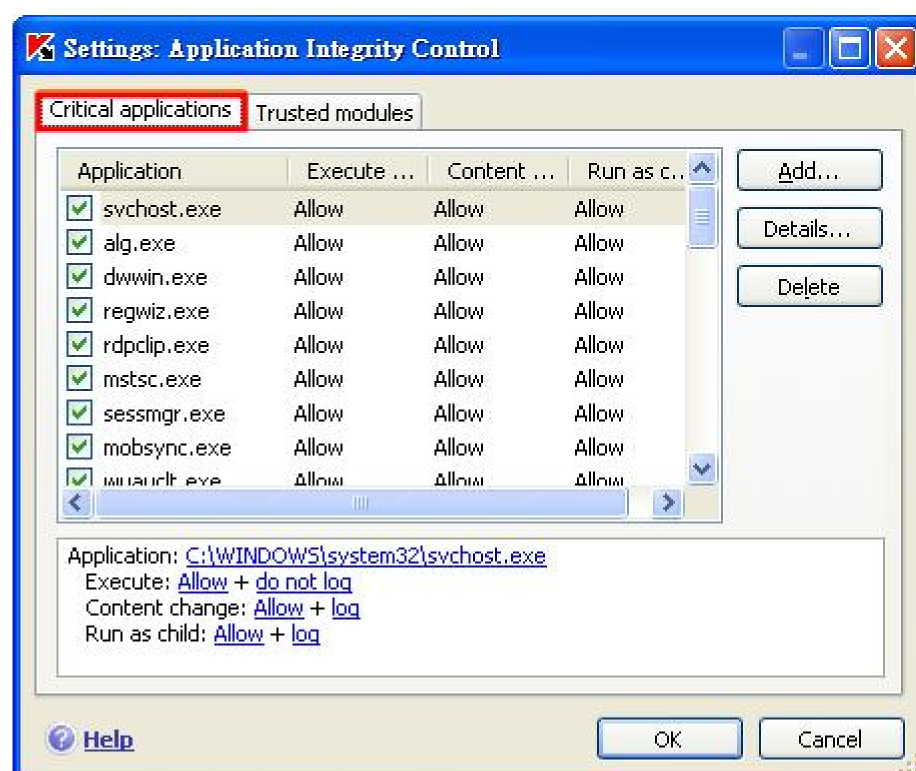
KIS 6 提供了先進的系統免疫防護，隨時監控系統的任何動作，避免有惡意行為的程式碼修改您的系統，危害系統的安全性，在免疫防護的內容當中，提供了四大監控機制如下圖



設定**應用程式活動分析器**：【Application Activity Analyzer】應用程式活動分析器可針對使用者在作業系統所安裝的應用程式做行為分析，不斷的監控是否有不安全的危險行為，提醒使用者是否允許執行，並留下系統記錄



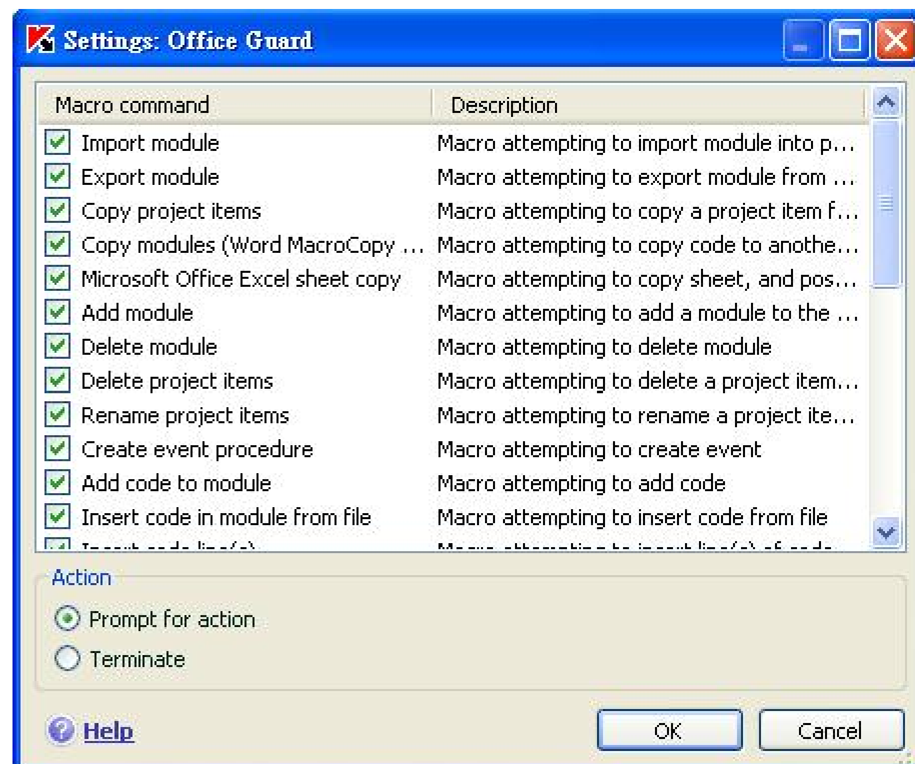
應用程式整合控制：【Application Integrity Control】可以監控所有正在記憶體中執行的程序，避免部某些惡意程式嵌入應用程式，導致危害系統安全性的行為，及可以選擇加入信任的模組【Trusted modules】



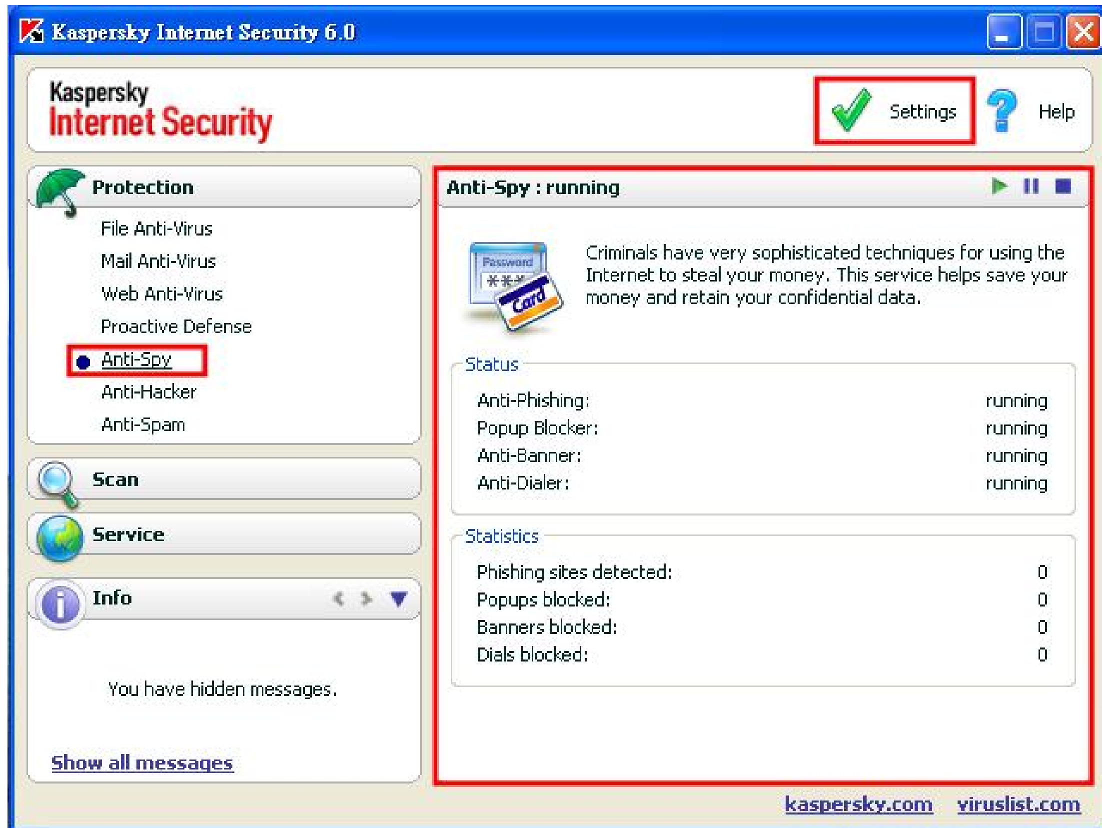
系統註冊檔保護：【Registry Guard】有非常多惡意程式的目標就是修改作業系統的註冊檔，威脅系統的安全性，例如：木馬病毒會透過對系統註冊檔的修改，獲得系統資源存取權，損壞作業系統的完整性



OFFICE **巨集防護**：(Office Guard)巨集防護會隨時監控 OFFICE 開啟文件時，偵測是否有隱藏危險的巨集指令，當巨集被載入時，巨集防護會提示一個警告視窗在螢幕上，提示使用者偵測到一個危險的巨集指令，讓使用者選擇予許或結束



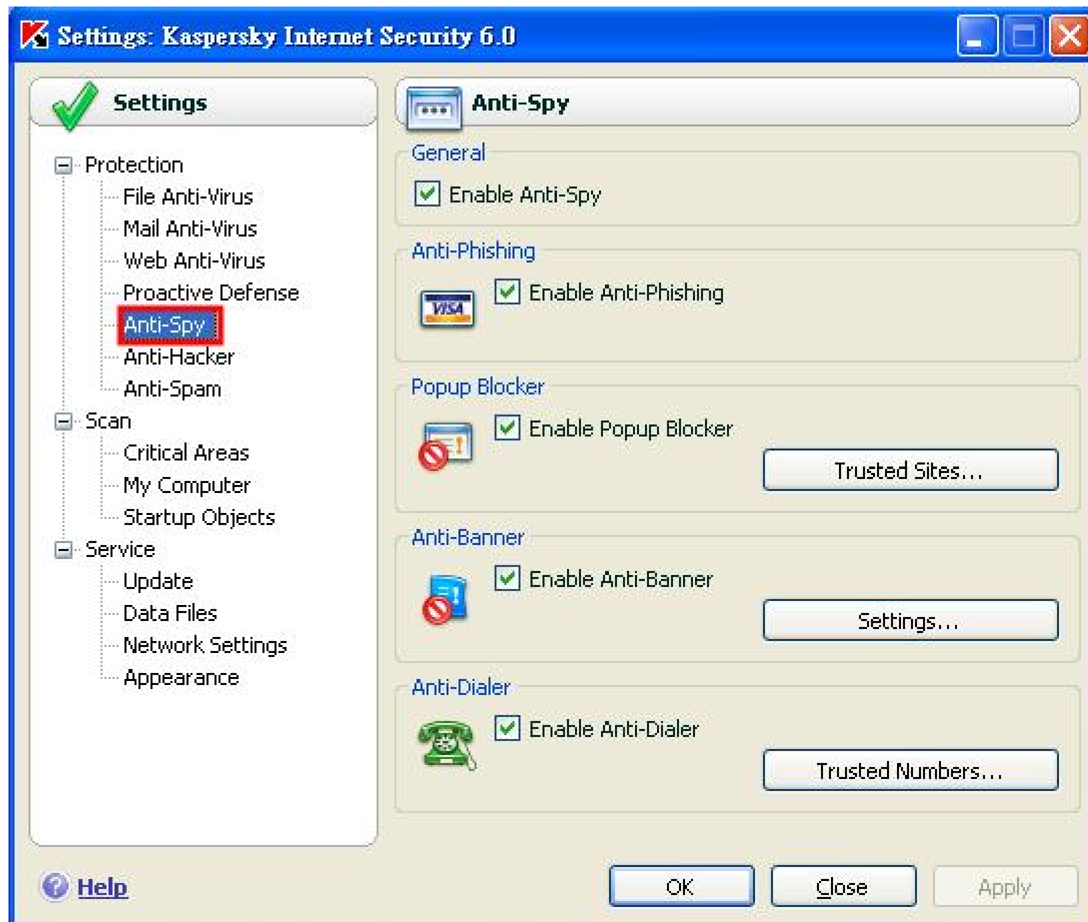
Anti-Spy (間諜程式防護)



釣魚程式(Phishing)及鍵盤側錄(keyloggers)主要用來偷取您的資料，自動撥號程式(autodialers)、玩笑程式(Joke programs)及廣告軟體(Adware)。則會浪費您的時間及金錢。Anti-Spy 就是被設定來保護您的電腦避免上述程式的干擾。

在「Anti-Spy」主畫面中，可以看到服務執行的狀態(status)及統計資訊(statistics)。如需要設定該功能項目，可點選「setting」進入設定畫面。

Settings- Anti-Spy (間諜程式防護)



至設定畫面中，勾選【Enable Anti-Spy】即可啟動 Anti-Spy 功能。

啟動【Anti-Phishing】: 即可啟動防護釣魚連結

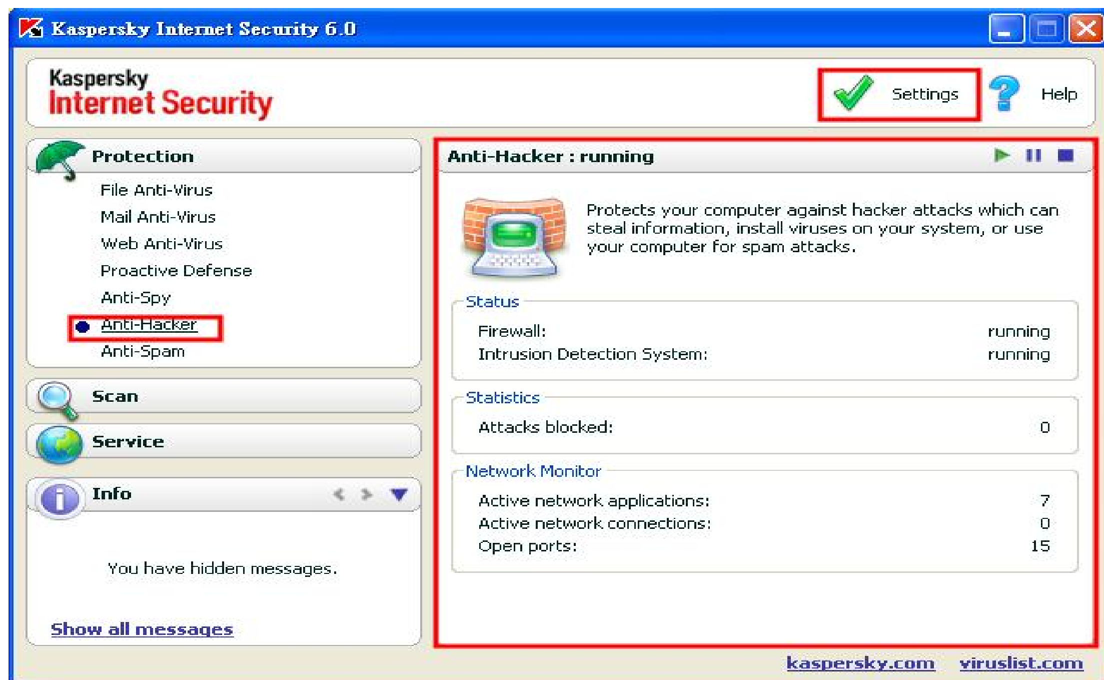
啟動【Popup Blocker】」: 即可阻擋蹦現視窗，亦可利用 Trusted Site…設定信任網址

啟動【Anti-Banner】: 即可阻擋 Banner 廣告視窗，亦可利用 Settings 設定黑白廣告名單。

啟動【Anti-Dialer】: 即可阻擋自動撥號威脅(Anti-Dialer)，

亦可利用 Trusted Numbers 設定信任撥號號碼

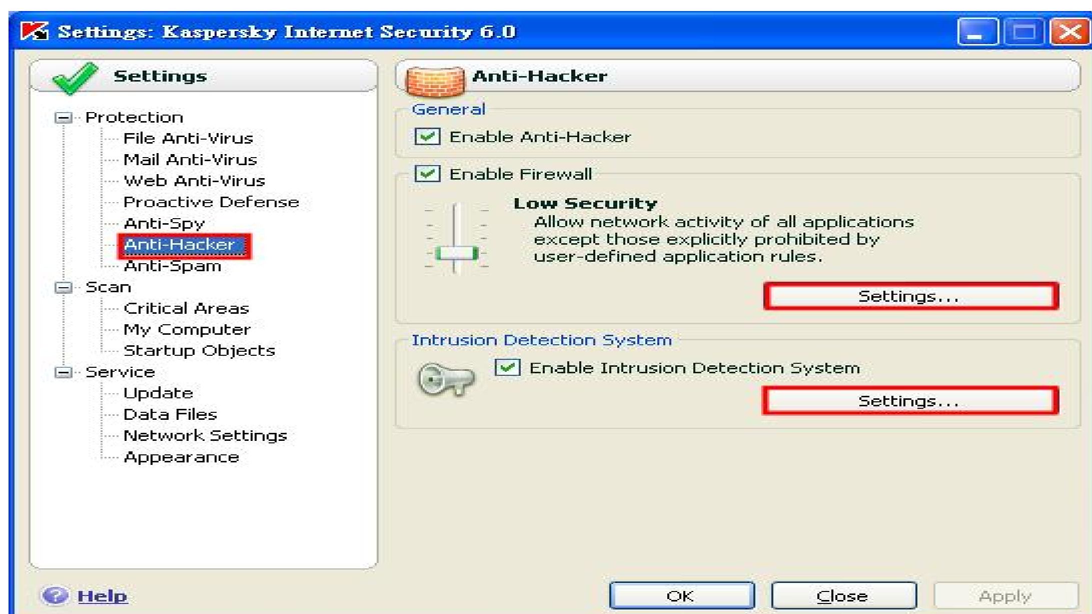
Anti-Hacker



Status：說明防火強還有IDS的執行狀況，Statistics：所阻擋的攻擊數量

Network Monitor：監控的應用軟體，連線，及接埠的數量

Settings- Anti-Hacker



General

　Enable Anti-Hacker：防火牆的開啟，Enable Firewall：防火牆的防護等級

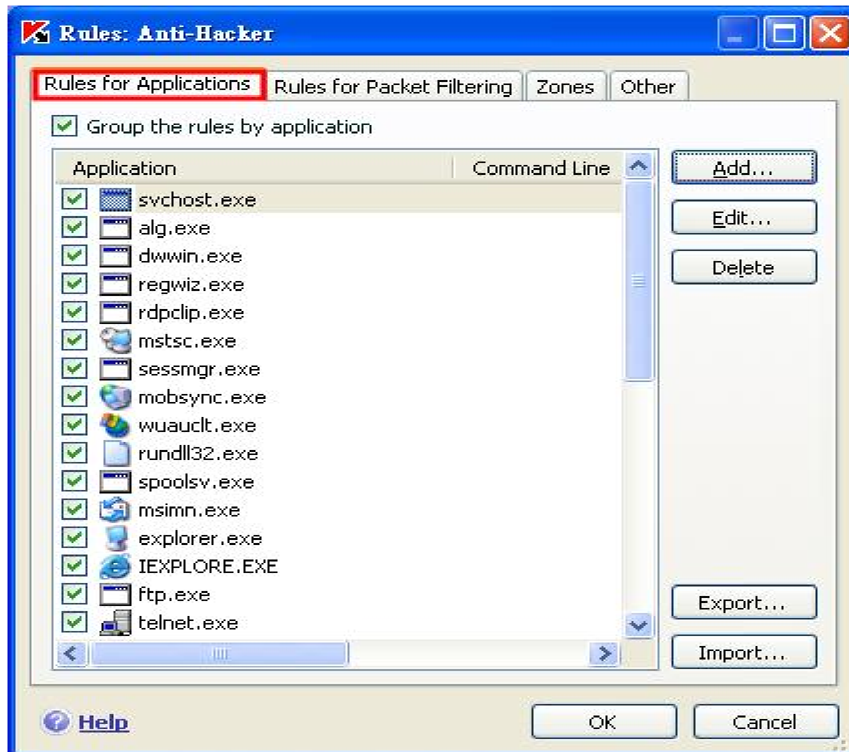
Intrusion Detection System

　Enable Intrusion Detection System：開啟IDS

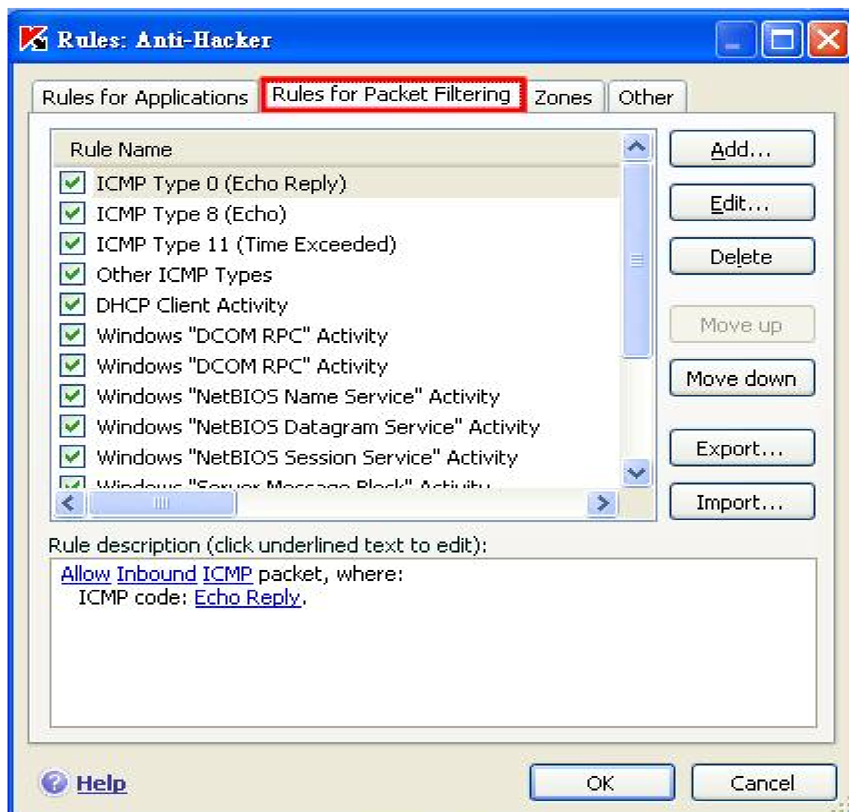
Anti-Hacker-Settings[Firewall]

Rules for Applications：設定應用軟體的規則

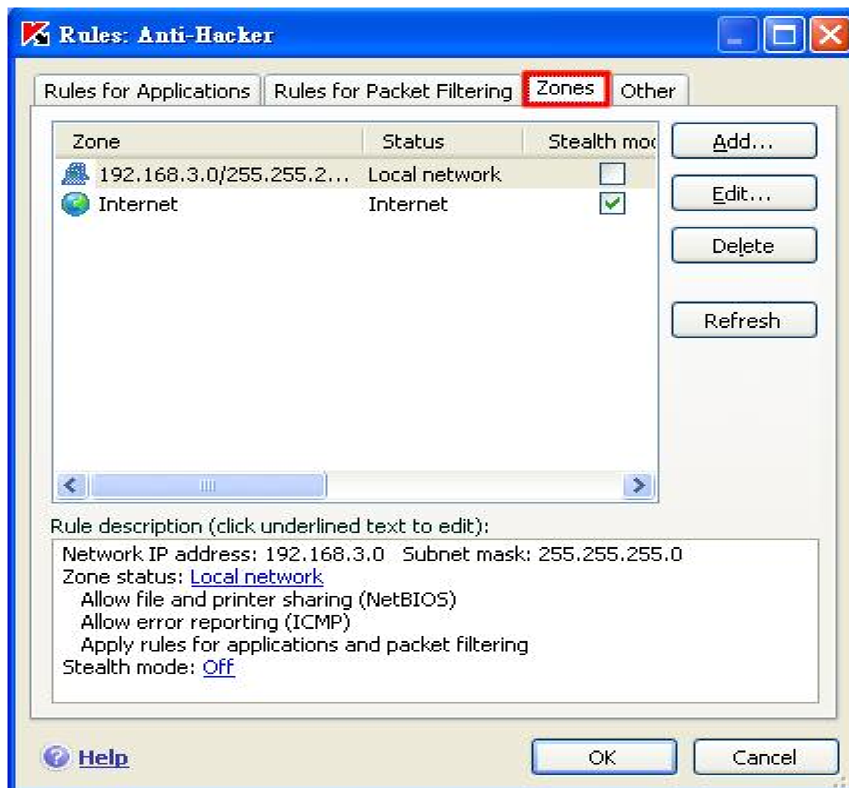
Group the rules by application：以應用軟體將規則劃分成同一個群組



Rules for Packet Filtering：封包過濾器的規則

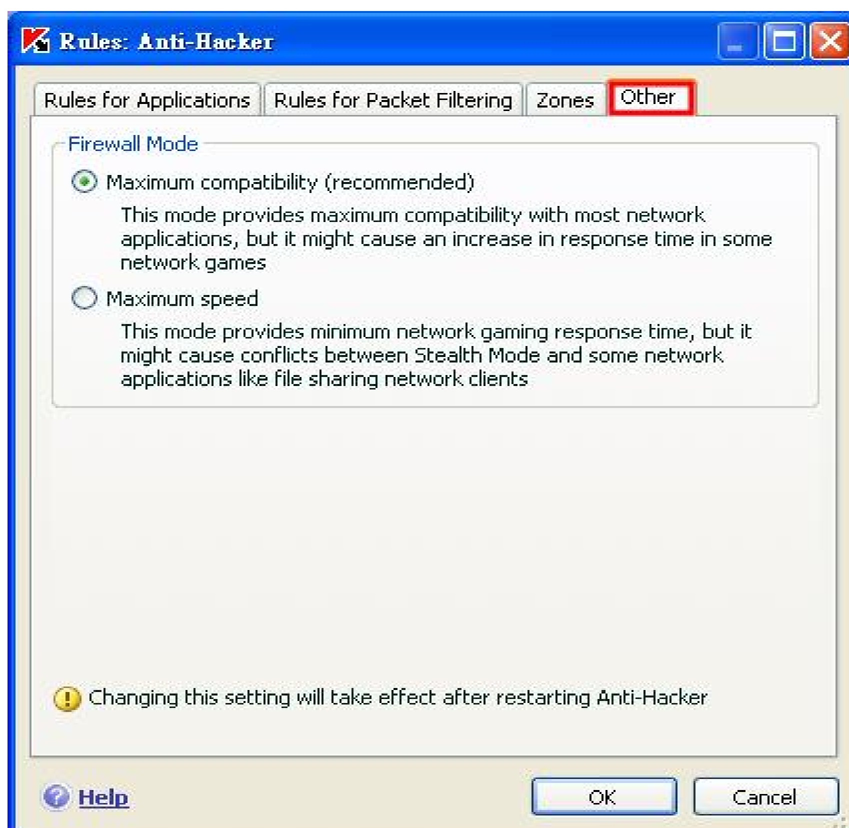


Zones：劃分網路範圍



Other Firewall Mode：防火牆模式

Maximum Compatibility：最大相容性，Maximum Speed：最高速度

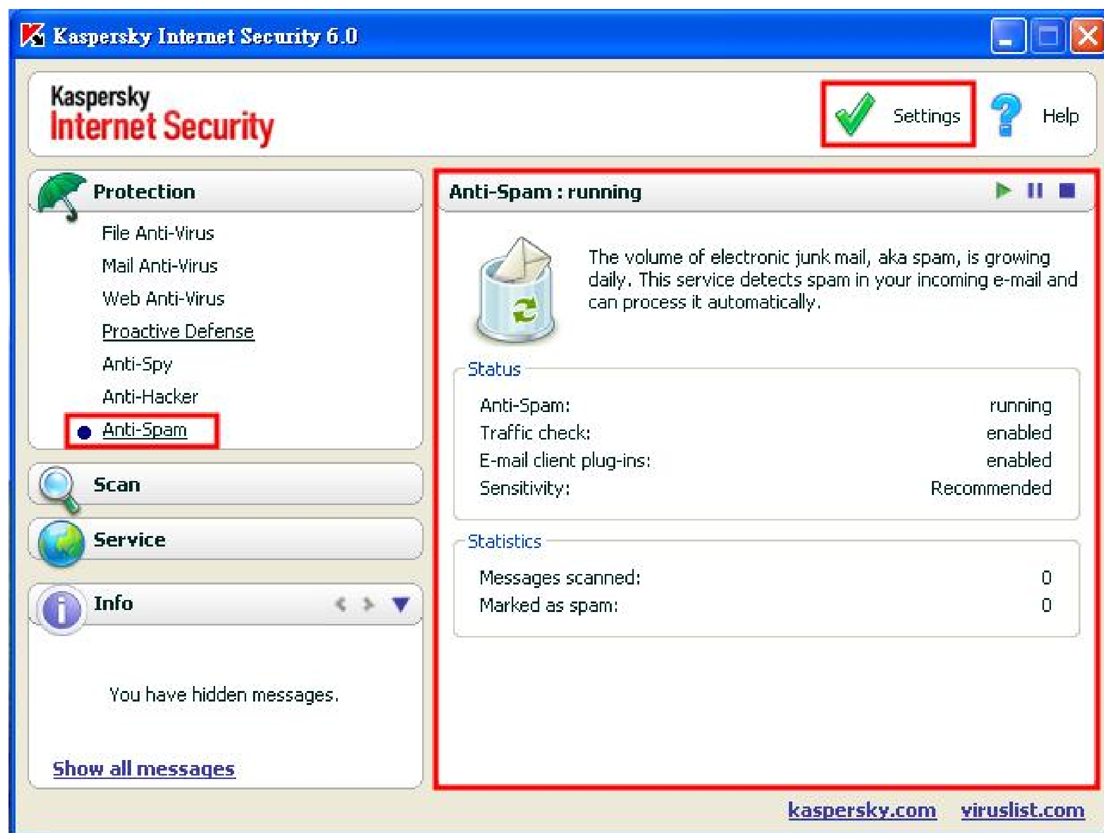


Anti-Hacker-Settings[Firewall]



Ban the attacking computer for：封鎖攻擊電腦的IP時間

Anti-Spam(垃圾郵件防護)

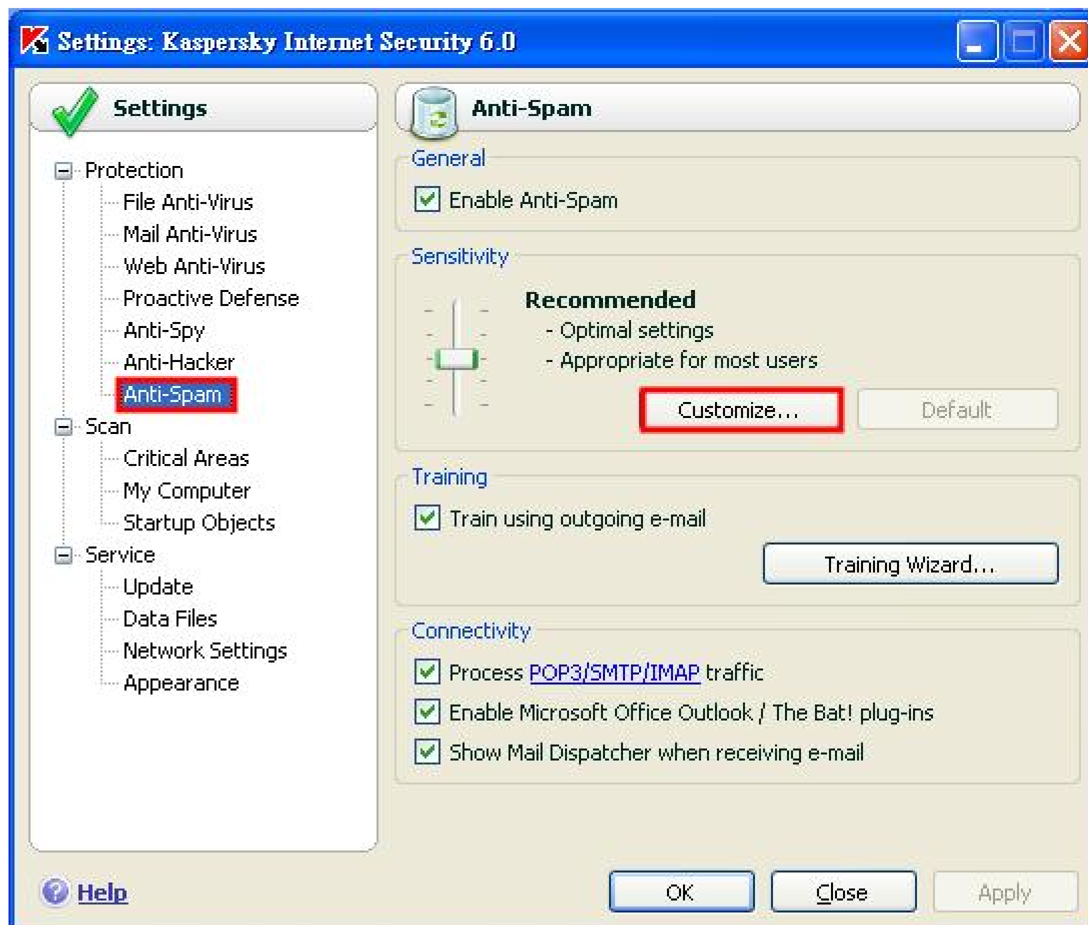


KIS 6.0 包含了一個可以偵測垃圾郵件及可制定過規則的元件，避免讓垃圾郵件影響了您收發 E-MAIL 的效率。

Status：Anti-Spam ， Traffic check ， E-mail client plug-ins Sensitivity 的流量掃描啟動顯示狀態

Statistics：顯示掃描 Messagess scanned 以及 標記為 Mark as spam 的數量

Settings-Anti-Spam(**垃圾郵件防護**)



Gerneral：使用者可以選擇開始或關閉垃圾郵件防護的功能

Sensitivity：使用者可以設定垃圾郵件防護層級，來做垃圾郵件過濾的規則，或可選擇自行定義一個過濾的機制，以符合使用者的需求（自訂內容請參見下一頁）

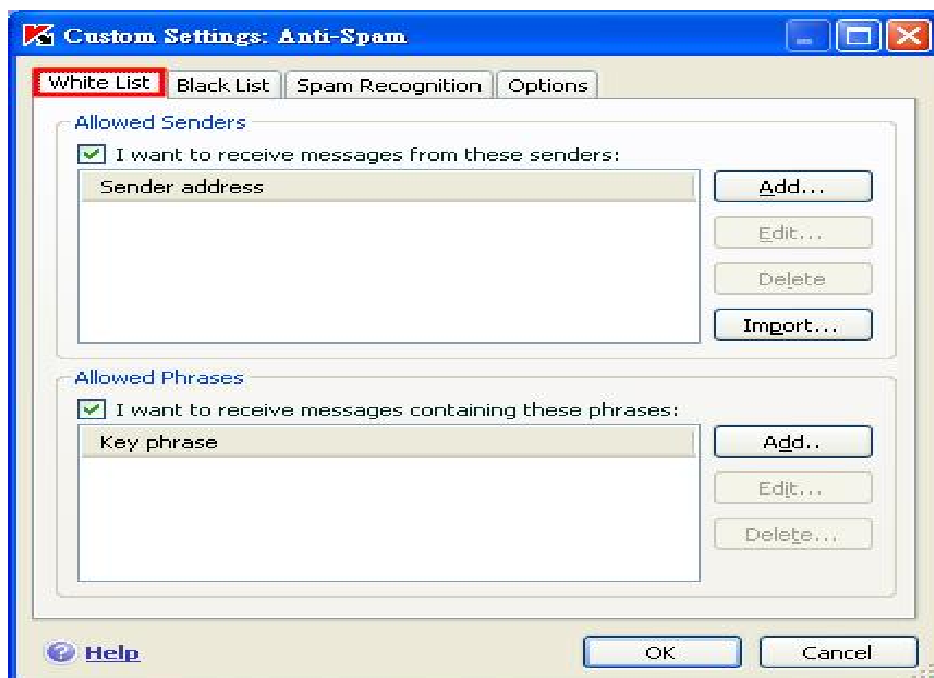
Training：垃圾郵件防護整合了 Microsoft Outlook 、Microsoft Outlook express 和 The Bat!，可透過收件匣來訓練垃圾郵件的過濾機制

Connectivity：可以設定處理電子郵件通訊協定（POP3/SMTP/IMAP）的流量，和是否使用 Microsoft Office Outlook / The Bat!的擴充模組根據您的分析狀態來設定訊息的處理規則。以及使用者可在從郵件伺服器下載前，進行所有內送電子郵件的訊息標題做初步分析，可減少下載到您電腦的垃圾信與病毒的風險

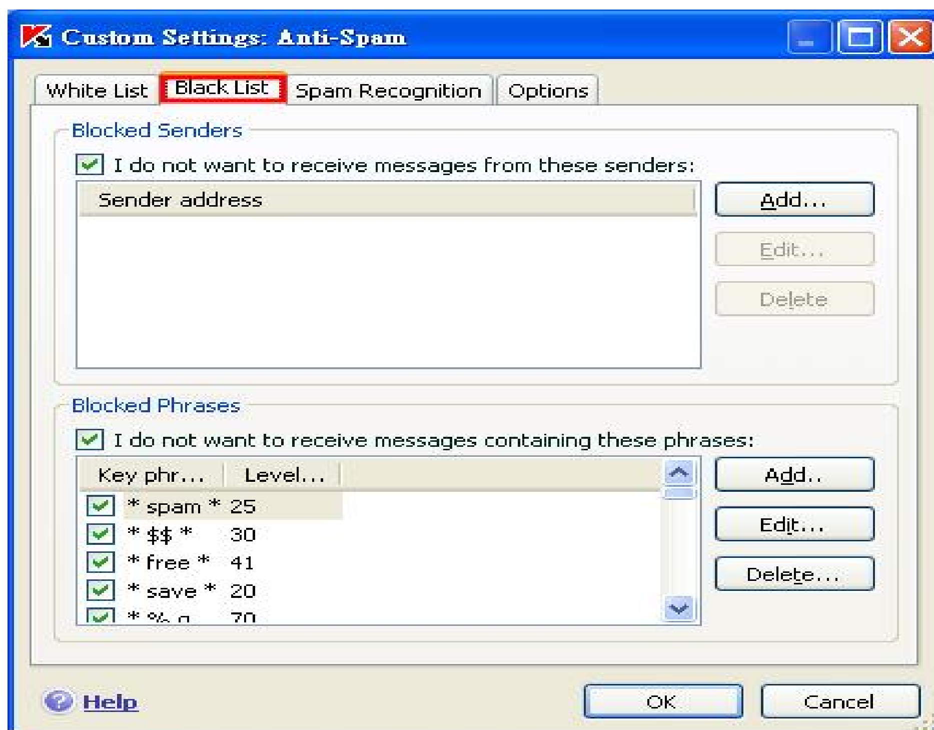
Anti-Spam(**垃圾郵件防護**)-Customize

自訂郵件過濾規則

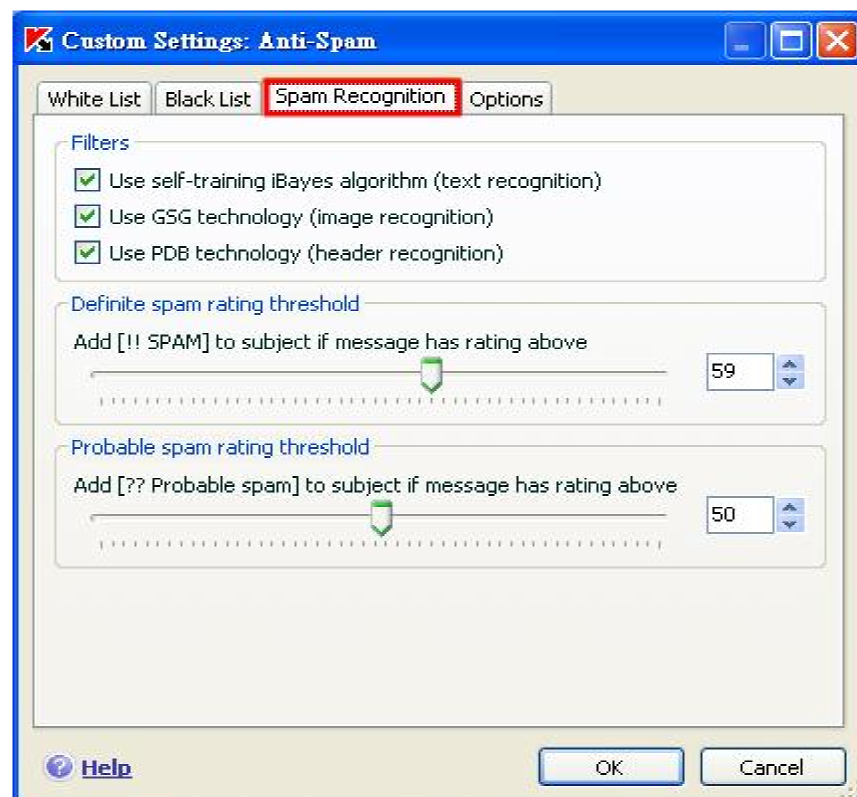
使用者可自行定義寄件者【白名單 Sender address】，以及設定允許信件標題或內容訊息【文字的片語 Phrases】清單



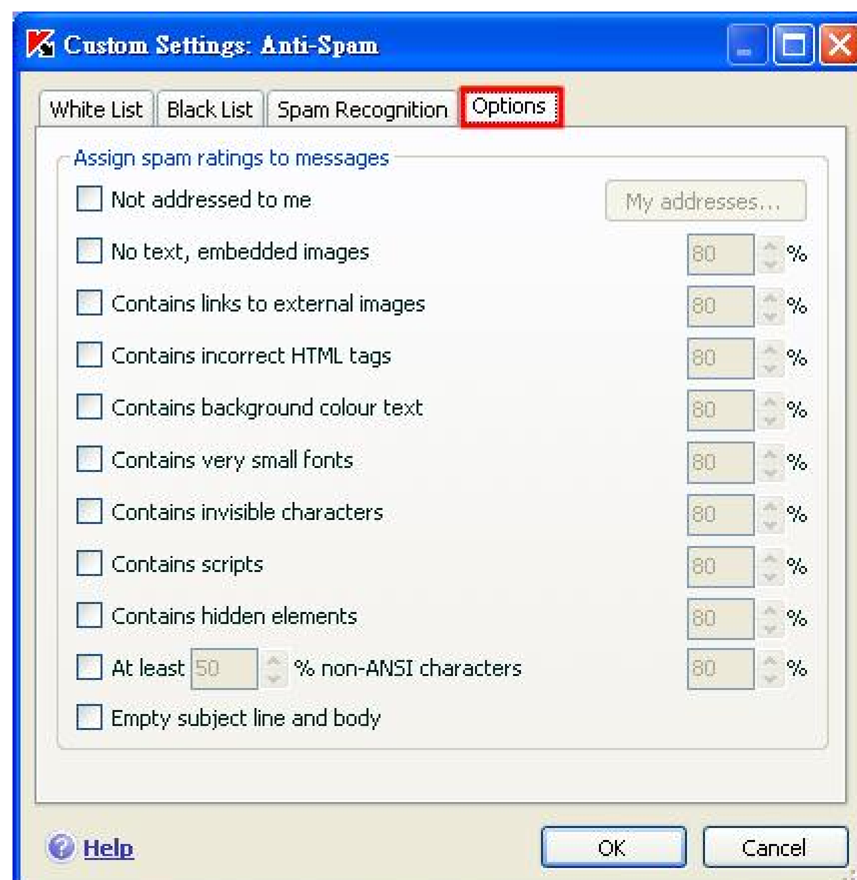
本設項目可針對垃圾郵件設定寄信【黑名單 Black List】，以及封鎖信件標題或內容訊息【文字的片語 Phrases】清單。



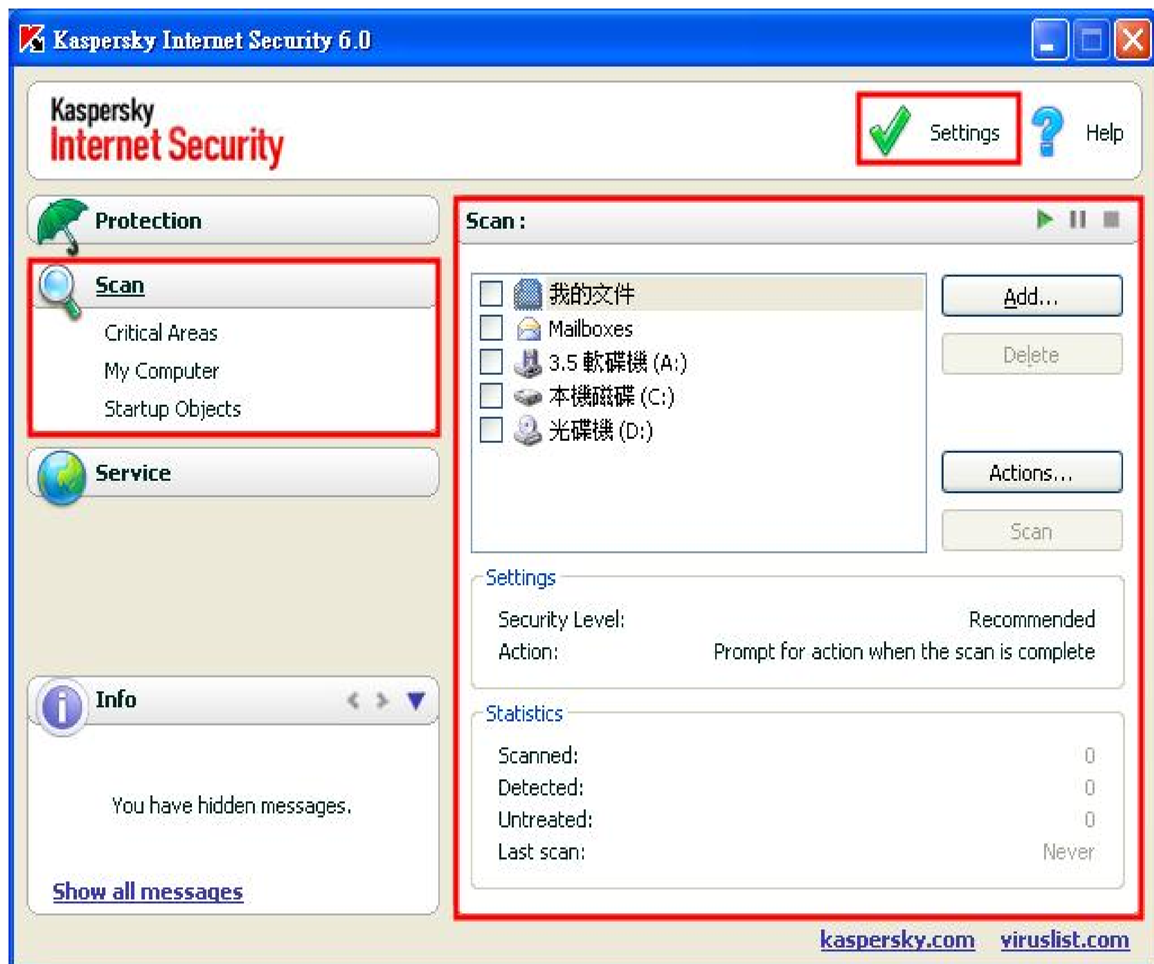
垃圾郵件辨視率：



調整選項：



Scan (**檔案掃描**)



檔案掃描功能可用來掃描指定磁碟機、資料夾、檔案及或做全機掃描。

如何設定及使用掃描工作：

卡巴斯基實驗室提供下列幾種掃描方式：

(1)掃描指定的區域：

可從掃描功能畫面的視窗自行選取及加入要掃描的物件。

按下「scan」即可開始掃描。

(2)Critical Areas：掃描嚴重區域(critical areas)

此區域為存放與系統檔案。

(3)My Computer：掃描我的電腦(My Computer)

掃描此電腦上全部之檔案

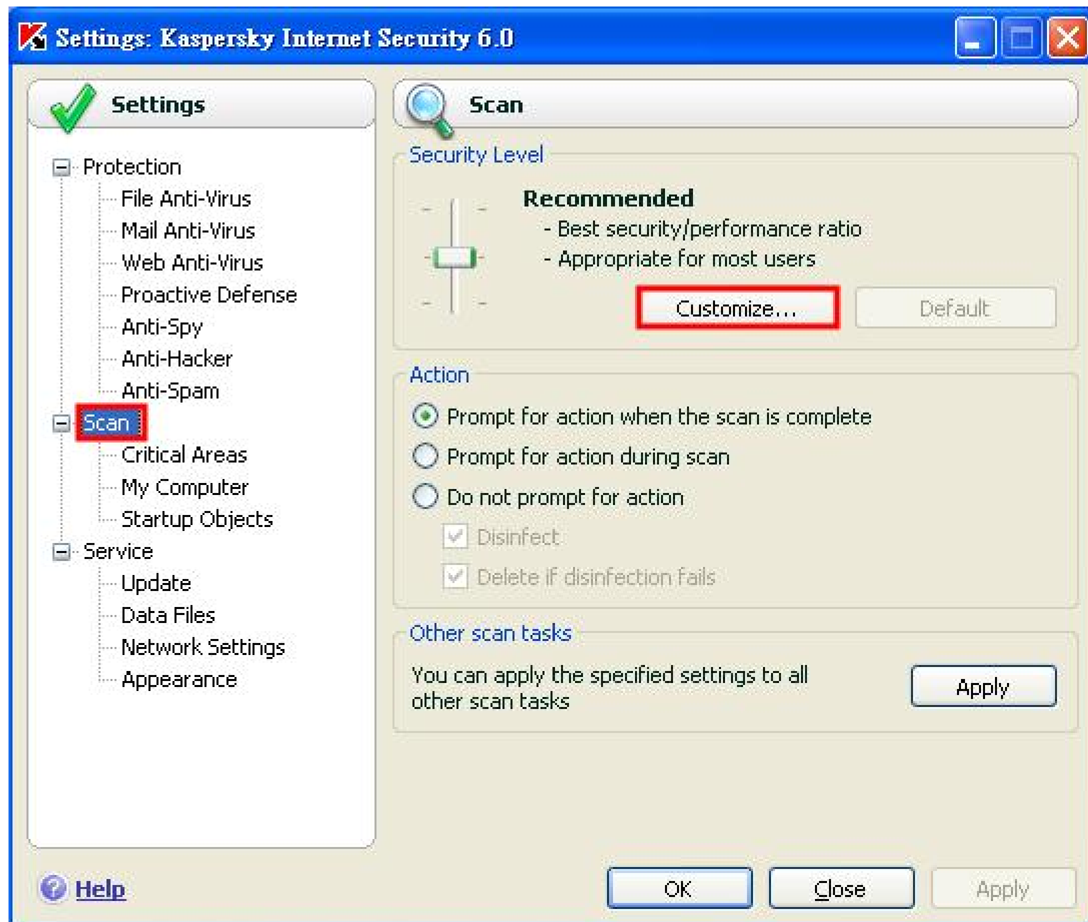
按下「scan」即可開始掃描。

(4)Scan Startup object：掃描啟動物件(Startup Objects)

掃描此電腦開機時會用到的物件內容。

按下「scan」即可開始掃描。

Settings- Scan (**檔案掃描**)



Security Level:

檔案掃描的等級：預設為建議(Recommended)。

Action：掃描時的執行動作

Prompt for action when the scan is complete：掃描完成後再詢問病毒處理動作

Prompt for action during scan：掃到病毒時就詢問使用者處理動作

Do not prompt for action：不要出現處理病毒提示畫面

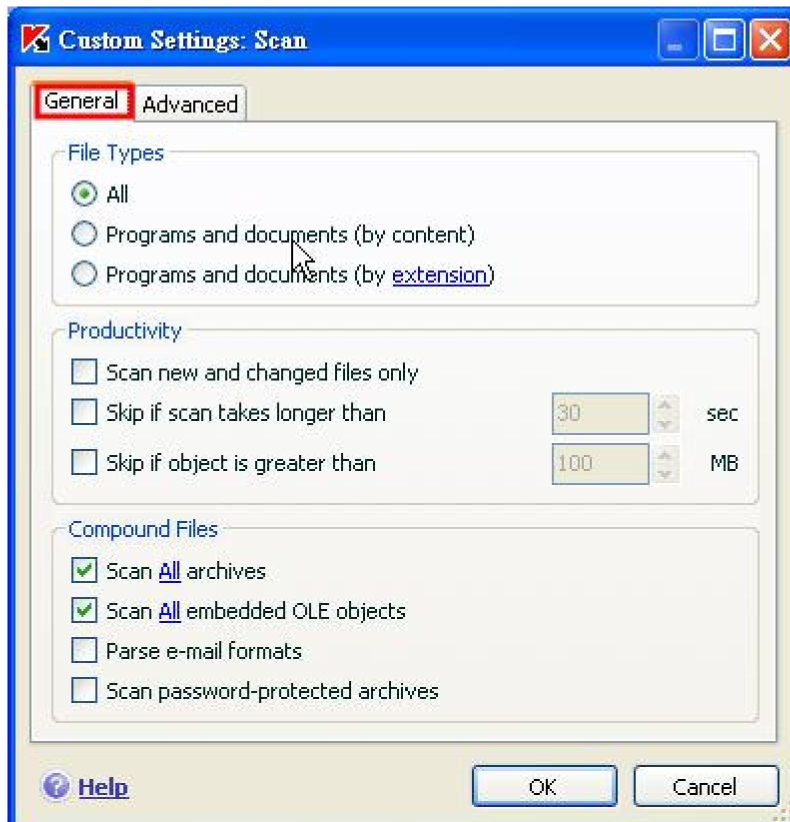
Disinfect：清除病毒

Delete if disinfection fails：如果掃描到病毒則清除病毒，如果無法清除病毒則刪除檔案

Run Mode

Every 1 Day(s)：每隔多久執行預定的掃描

Scan (**檔案掃描**)-Customize[General]



File Types：掃描檔案格式

All：掃描全部檔案

Programs and documents (by content)：只掃描檔案內容可能會被感染的檔案

Programs and documents (by extension)只掃描可能被感染的檔案格式。

Productivity：可在此調整掃描效率

Scan new and changed files only：只掃描新建立及被修改過的檔案

Skip if scan takes longer than：設定掃描檔案超過設定秒數時則忽略

Skip if object is greater than：設定檔案大小超過設定大小時則忽略

Compound Files：複合式檔案設定

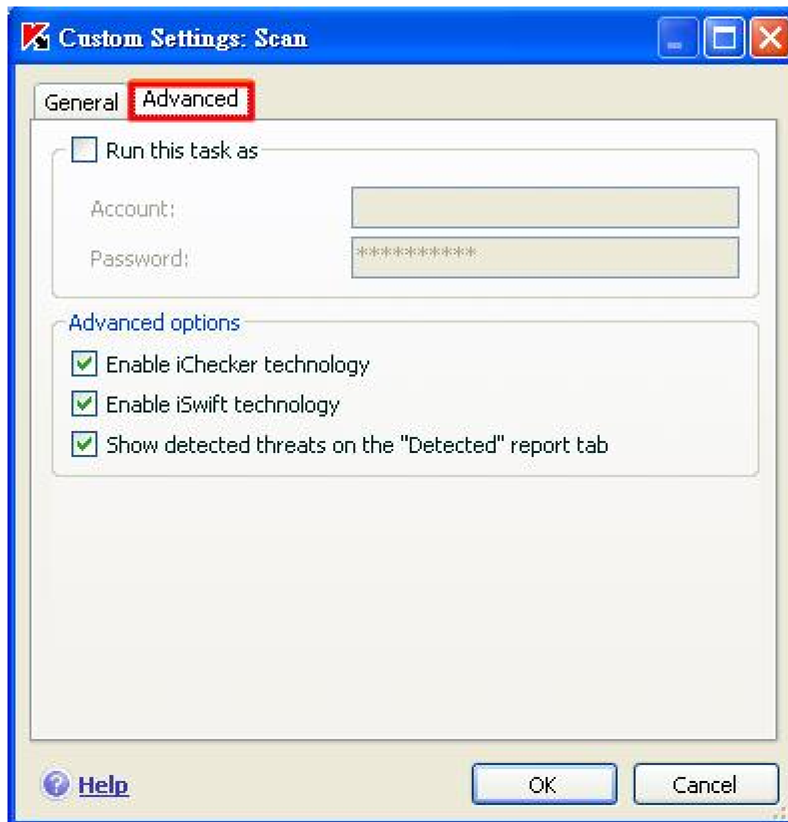
Scan All archives：預設為掃描全部的封存檔案

Scan All embedded OLE objects：預設為掃描全部的嵌入式物件

Parse e-mail formats：掃描郵件資料庫檔案

Scan password-protected archives：掃描密碼保護檔案

Scan (**檔案掃描**)-Customize[Advanced]



Run this task at：使用指定帳號執行掃描工作

  Account：帳號

  Password：密碼

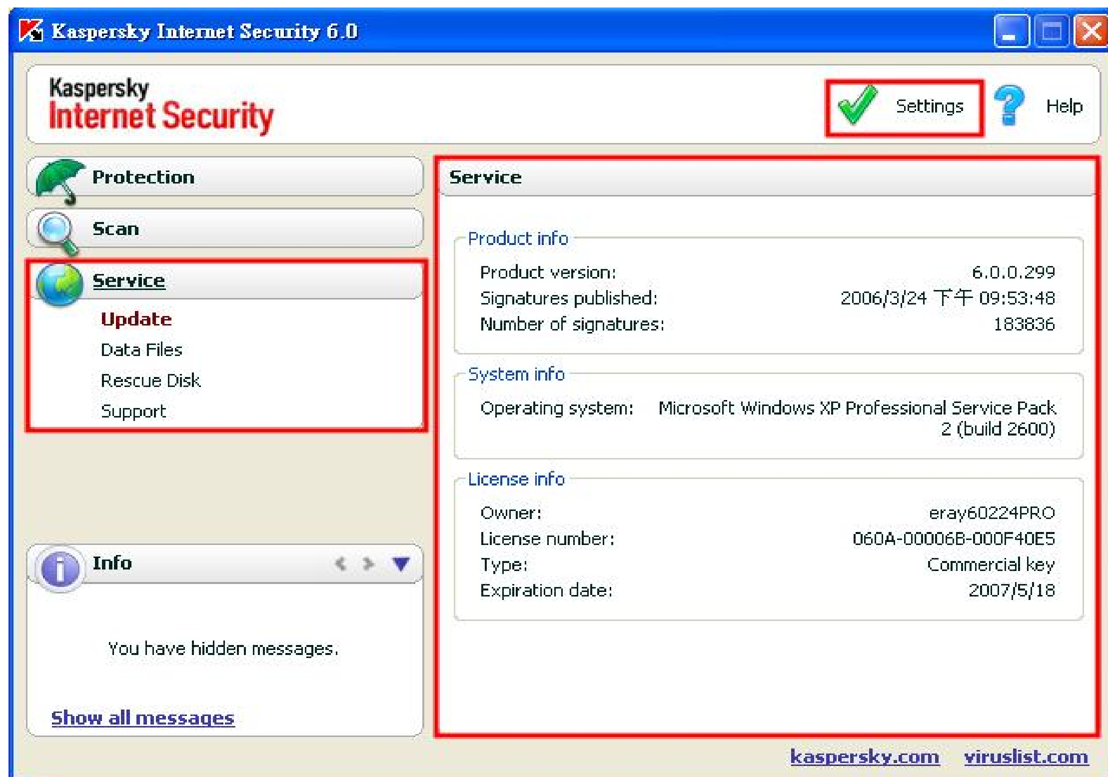
Advanced options：其他選項

  Enable iChecker technology：啟用 iChecker 技術

  Enable iSwift technology：啟用 iSwift 技術

  Show detected threats on “Detected” report tab：將偵測到的病毒顯示在”Detected”報表中

Service



Product info

Product version:產品版本

Signatures pulished:已發布最新簽署

Number of signatures:簽署數目

System info

Operating system:作業系統

License info

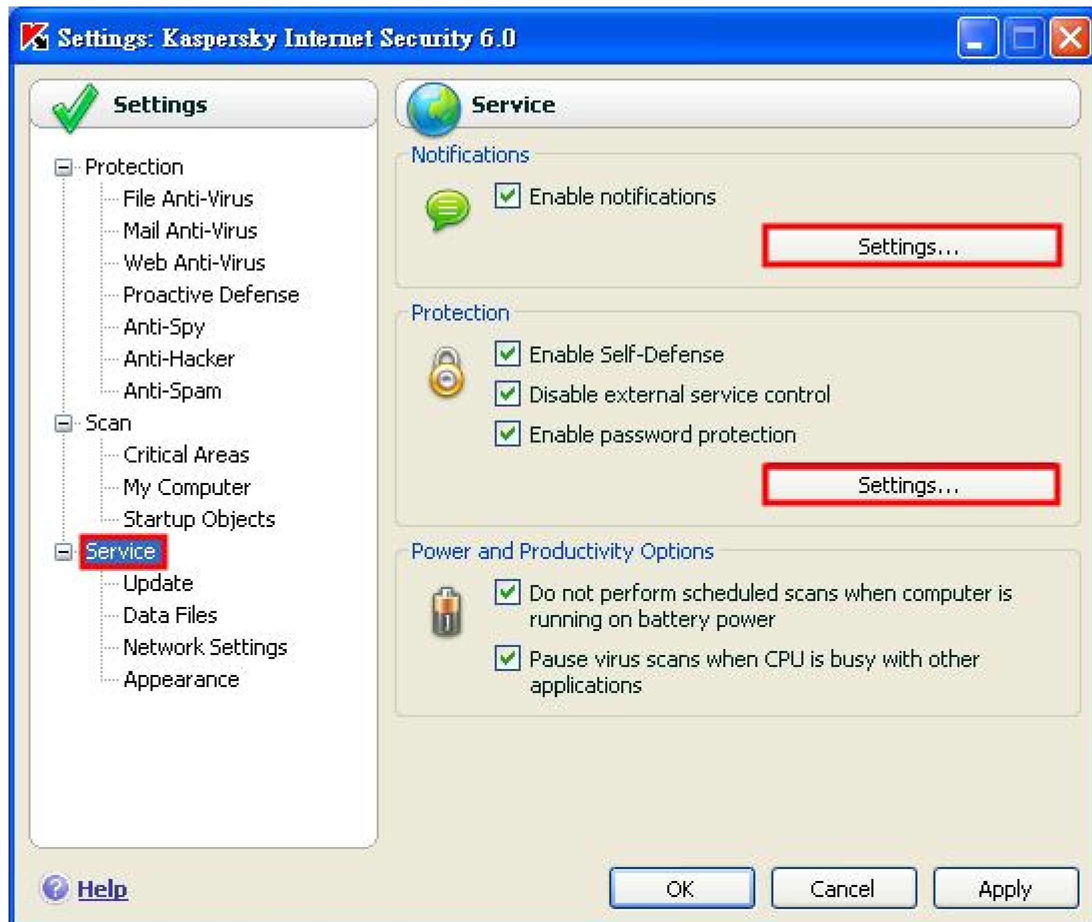
Ower:授權擁有者

License number:授權號碼

Type:授權形式

Expiration date:授權到期日期

Setting -Service



Notification

Enable notifications:允許事件提示，setting 中可以設定提示的事件，也可以設定提示的電子信箱，及提示的頻率

Protection

Enable self defense：保護系統檔案不被刪除或是更改

Disable external service control：禁止外部的控管或是連結

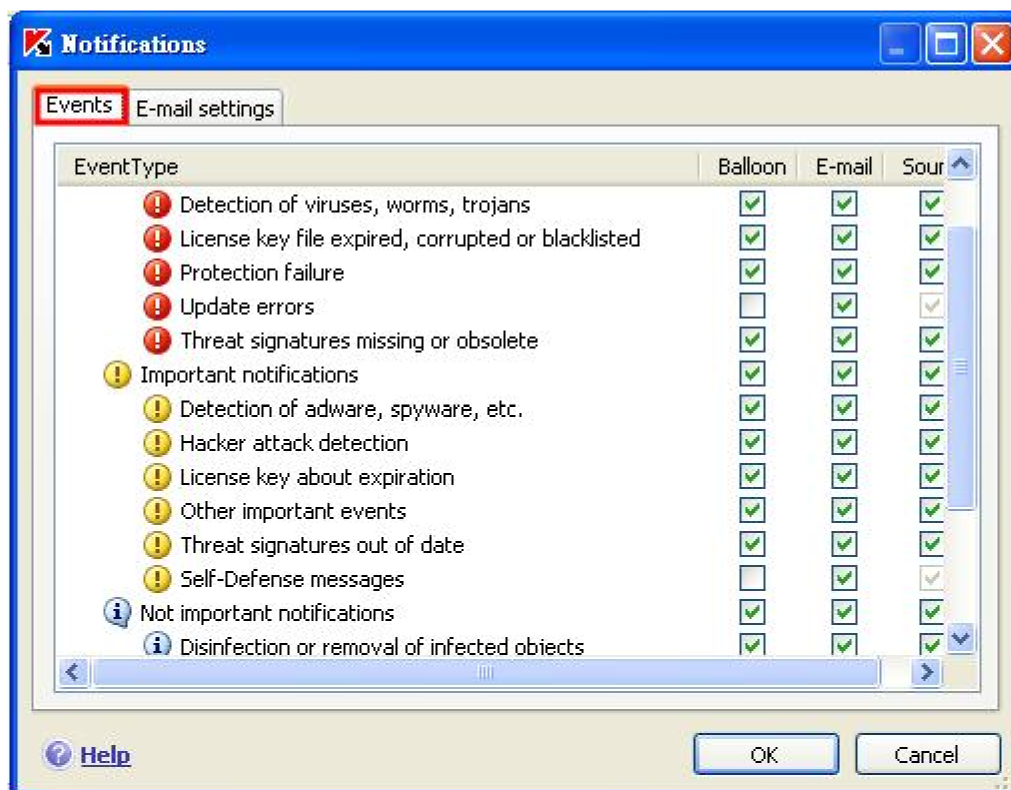
Enable password protection：設定反安裝密碼

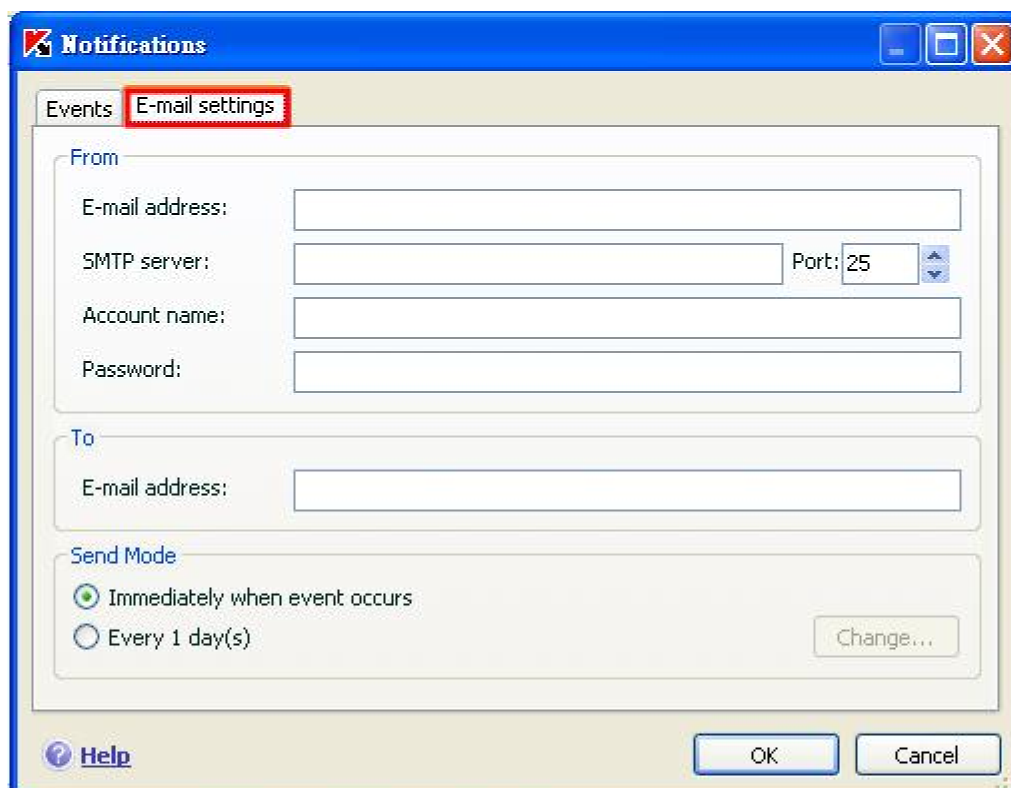
Power and Productivity Options

Do not perform scheduled scans when computer is running battery power：當電腦是使用電池時，不實行行程上的掃描

Pause virus scan when CPU is busy with other applications：當 CPU 在執行其他應用程式時，暫停病毒掃描

Service-Settings [Notification]

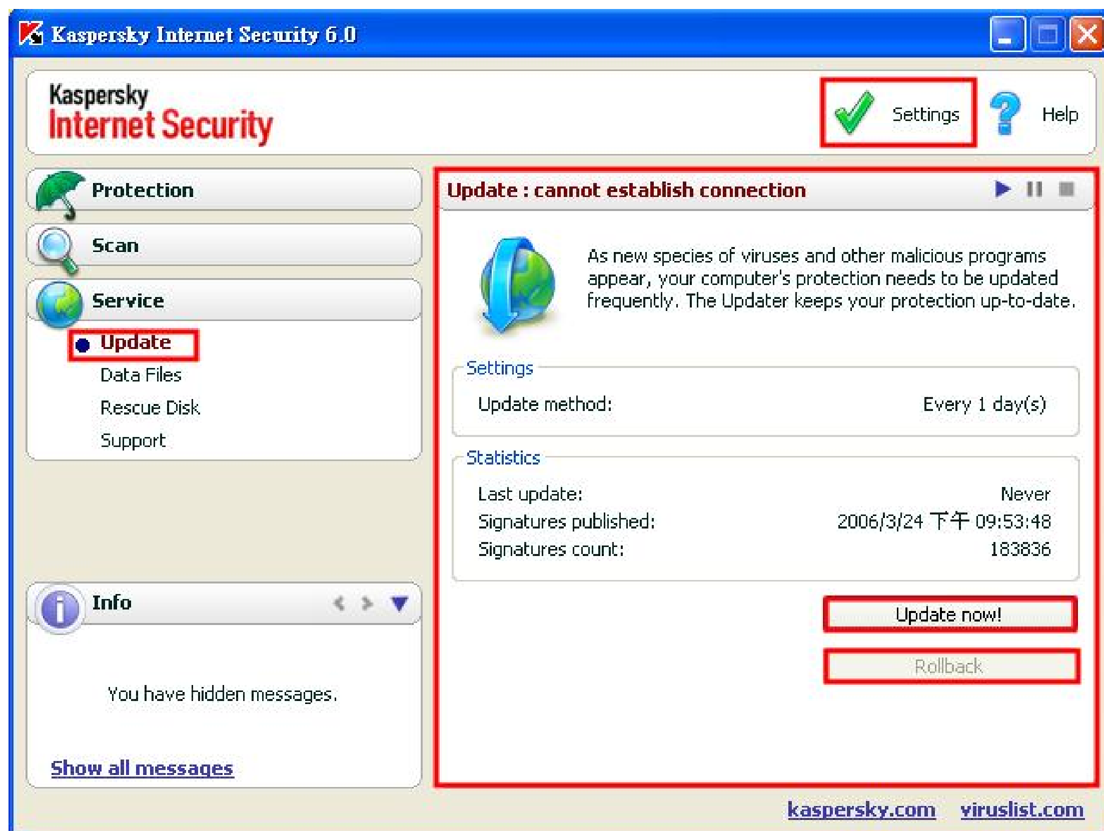




From：設定要從那個信箱寄出

To：設定要寄到那個信箱

Update



Settings

　Update method：更新方法

Statistics

　Last update：最近一次的更新日期

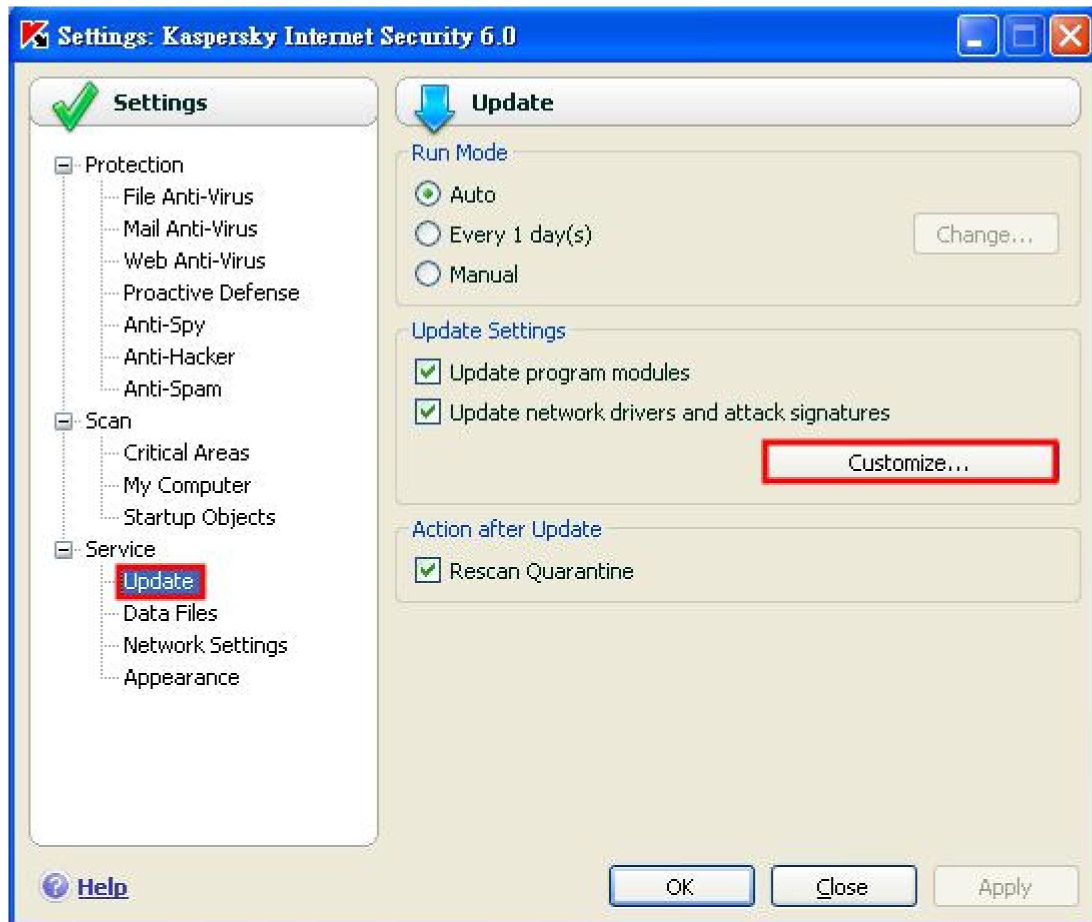
　Signatures pulished：簽署的日期

　Signatures counts：簽署的計數

Update now：立刻更新

Rollback：回復資料庫

Settings-Update



Run mode：執行的模式

Auto：自動

Every 1 day：每一天(這裡的時間可以在 Change 自行調整)

Manual：手動

Update setting：更新設定

Update program modules：更新程式模組

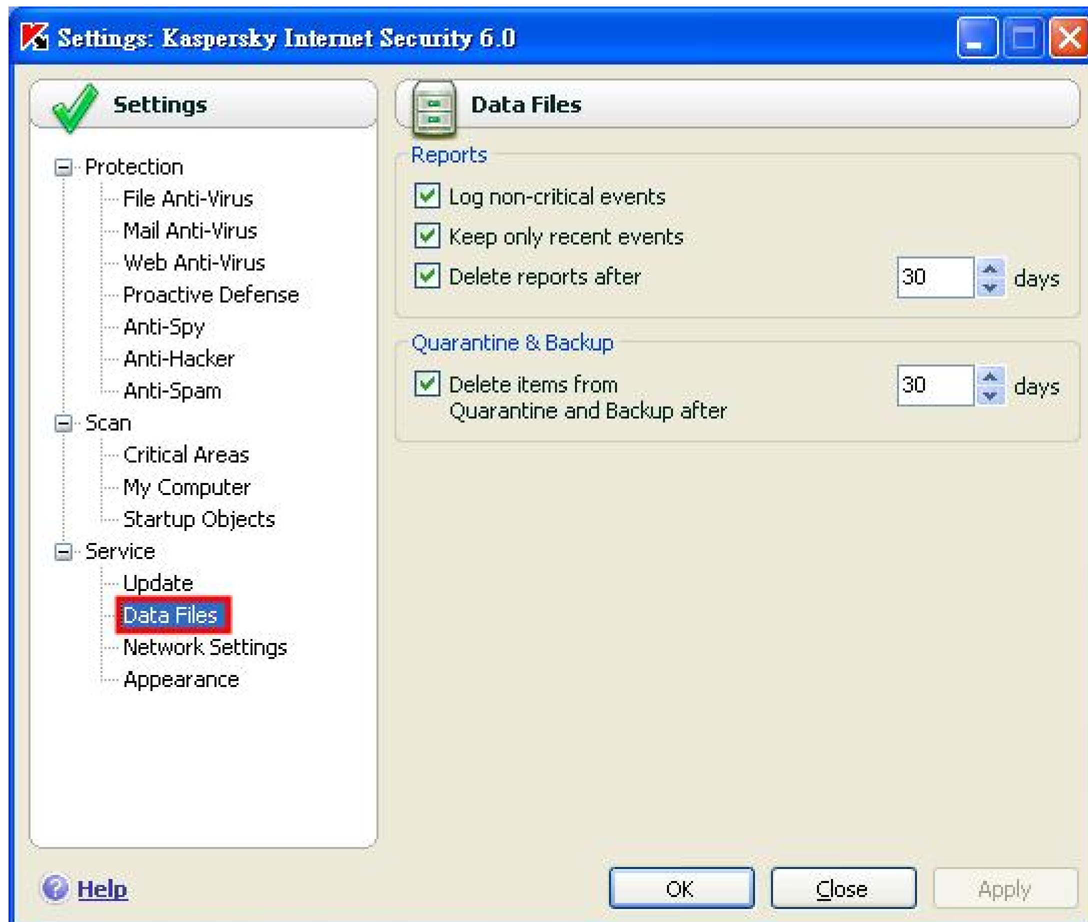
Update network drivers and attack signatures：更新網路驅動程式及攻擊簽署

Customise：可以設定區域網路設定、更新伺服器、其他

Action after

UpdateRescan quarantine：再次掃描隔離區

Data files



Reports：

Log non-critical events：紀錄所有細節的事件

Keep only recent events：保留最近的事件

Delete reports after：在幾天以後刪除檔案，這是可以自行調整的

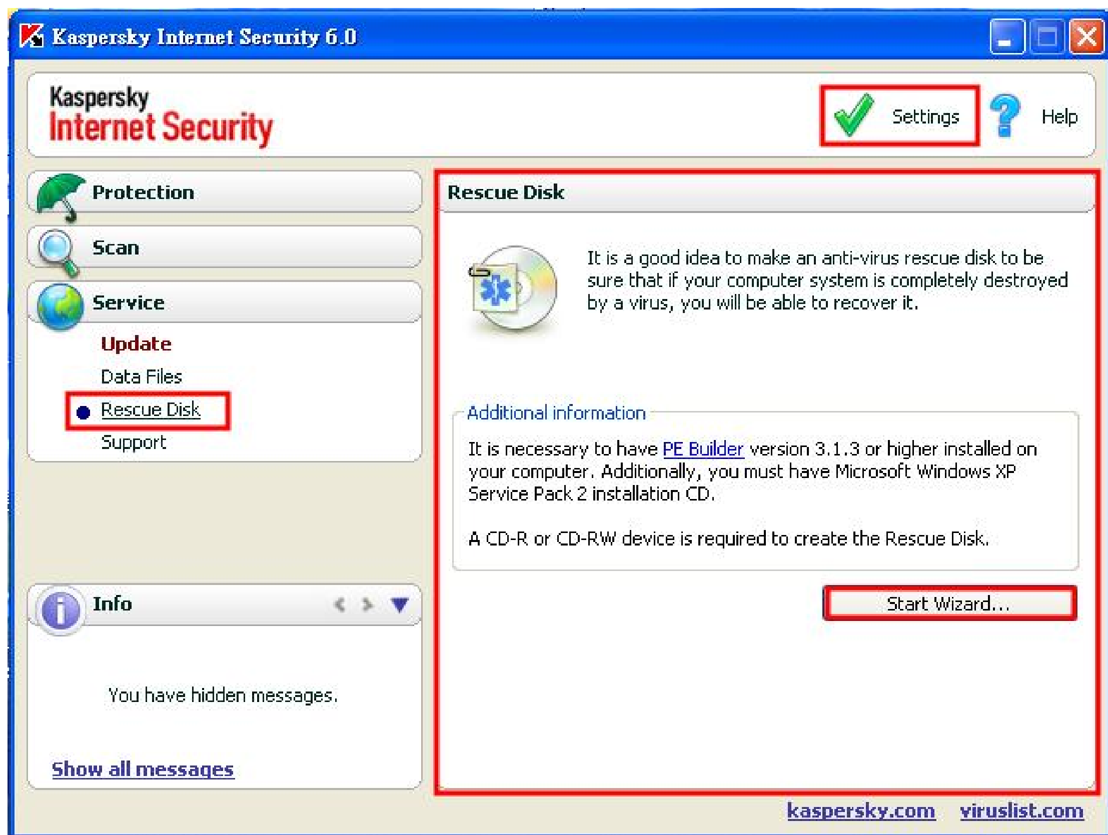
Quarantine

Delete items from quaratines and backup after：在幾天以後刪除隔離區及備份區的物件，時間可以自行調整

Backup：備份區，當受感染的檔案或是物件被刪除後，會儲存備份到此區

Clean up：清除 reports、Quarantine、Backup 的內容

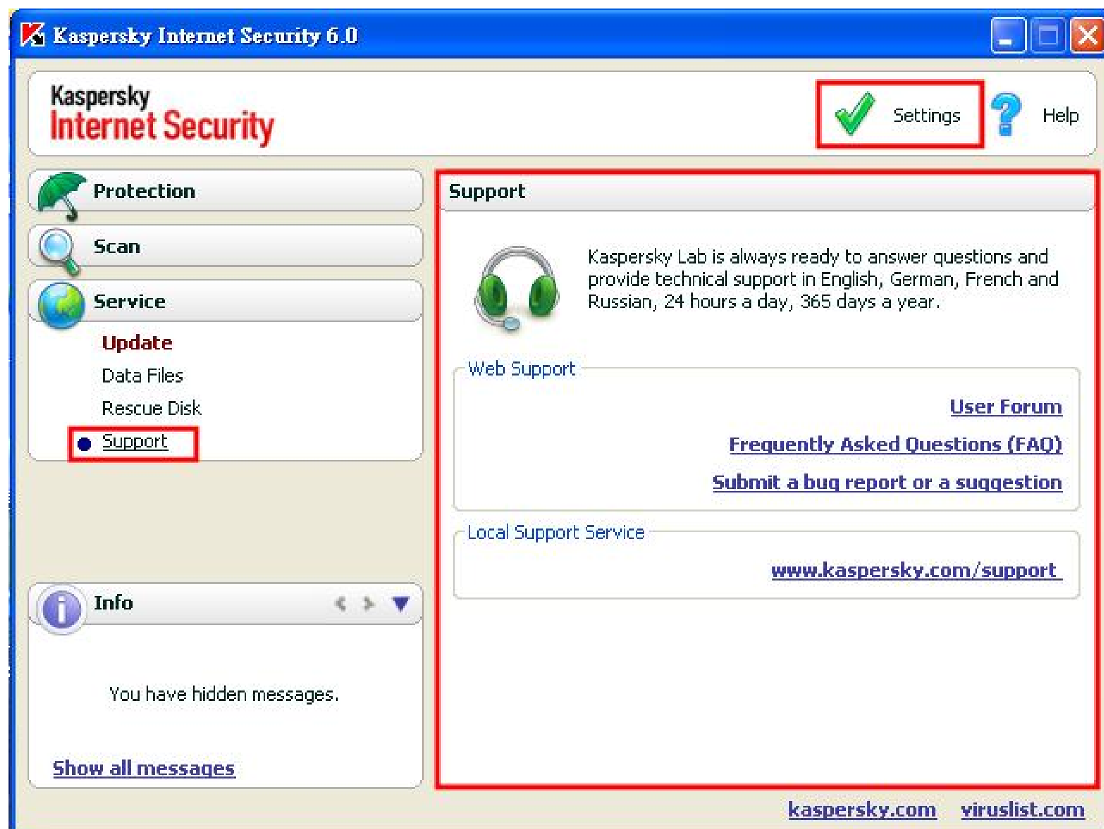
Rescue disk



您的電腦上需要安裝 PE builder 3.1.3 或是更新的版本，您也必須要有 windows xp service pack 2 的安裝光碟，也需要空白光碟或是空白 DVD。

Start wizard:還原光碟的開始精靈，分別需要輸入 PE builder 的資料夾位置、輸出的資料夾位置、是否使用之前已經儲存的檔案、windows xp service pack 2 安裝光碟的位置。

Support



Web Support

User forum：進入卡巴斯基論壇的網站

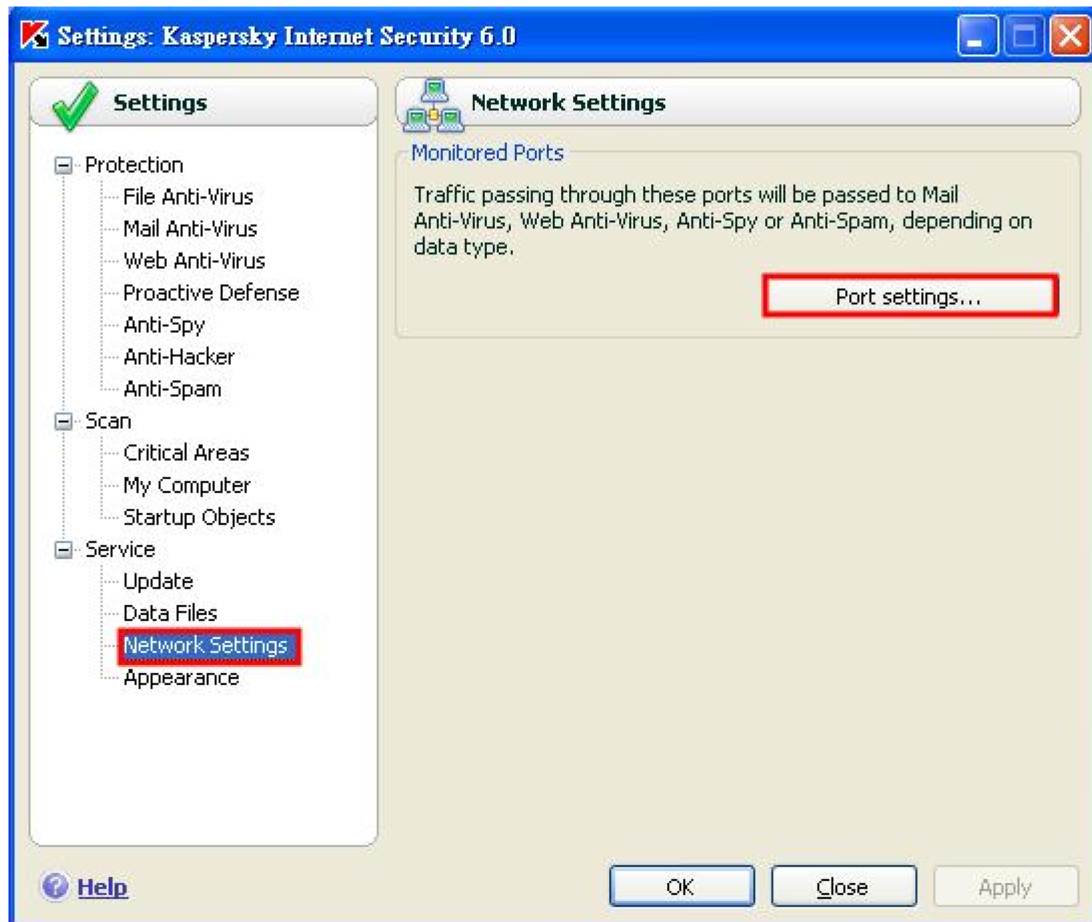
Frequently asked questions(FAQ)：進入卡巴斯基答客問的網頁

Submit a bug report or a suggestion：提交錯誤報告或是建議給卡巴斯基

Local Support Service

Local support service-www.kaspersky.com/support：進入卡巴斯基斯支援的網頁

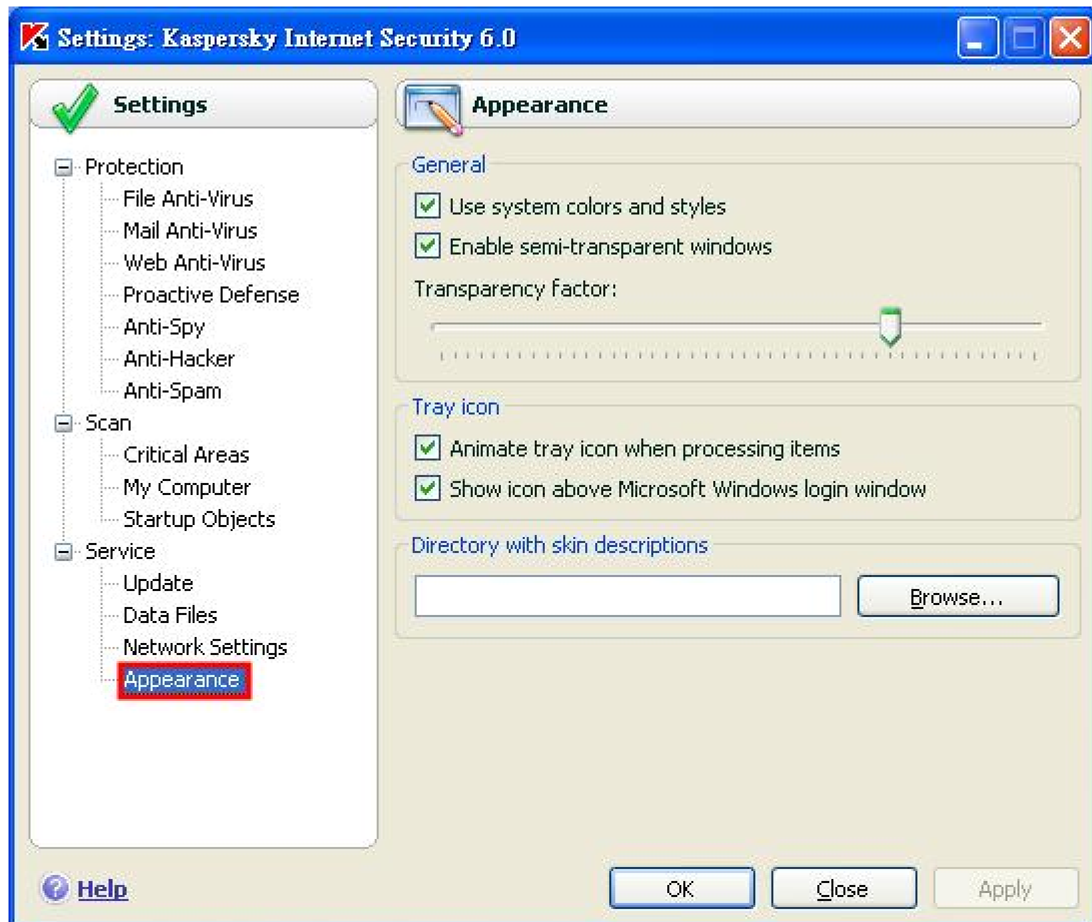
Settings-Network



Monitored Ports

Port setting：可以對想要監視的 PORTS 做增加、編輯、刪除的動作

Settings-Appearance



Genreral

Use system colors and styles：讓卡巴斯基的視窗跟系統的顏色及風格一致

Enable semi-transparent windows：是否使用半透明的視窗功能

Transparency factor：半透明的程度

Tray Icon

Animate tray icon when processing items：當處理物件時，是反讓右下角的小圖示即時呈現目前的狀態

Show icon above Microsoft Windows login window：是反在微軟登入視窗上方顯示卡巴斯基小圖示

Directory with skin descriptions

Directory with skin description：指向特定外殼的資料夾